解決方案簡介

網路最佳化的
第 5 代 Intel® Xeon® 可擴充處理器
機密運算

利用 HashiCorp Vault 與 Intel® Trust Domain Extensions (Intel® TDX) 進行祕密資訊管理

HashiCorp Vault 保護和管理私有加密金鑰、憑證和其他祕密資訊，減少網路安全功能的攻擊面。透過 Intel® TDX 硬體保護，Vault 與其他虛擬機器 (VM) 和系統軟體進一步隔離並受到保護。Intel® TDX 現已全面支援第 5 代 Intel® Xeon® 可擴充處理器。

網路安全的複雜性和成本比以往都更高，未能成功抵禦攻擊的潛在損害也比以往都更高。IBM 報告指出，2023 年資料外洩的全球平均成本已達到 445 萬美元，此數據在過去三年中成長了 15.3%，並繼續增加[1]。對企業來說，這些威脅的緊迫性和規模不僅使遵循最佳實務變得勢在必行，而且在保護重要核心資料時也必須盡可能創新。事實上，51% 的組織報告宣稱他們因為資料外洩，正在規劃新增安全投資[1]。

許多公司希望透過在營運中增加使用資料加密技術，以適度的成本和中斷來提高安全態勢。零信任網路存取 (ZTNA) 和安全存取服務邊緣 (SASE) 等安全導向的網路解決方案也正在普及，進一步增加加密技術的使用。因此，祕密資訊管理系統變得比以往都更加重要，為私有加密金鑰和其他憑證 (例如密碼和憑證) 的儲存提供保護。在所有這些情況下，對靜態和傳輸中的資料進行加密會減少攻擊面並有助於保護敏感資料。

即便如此，包括加密金鑰和其他祕密資訊在內的資料在使用時通常並未加密，因此很容易受到潛在的損害。在共用記憶體空間中暴露此類祕密資訊的流程通常使用軟體措施相互隔離，但這些流程可能容易受到權限升級攻擊，並且在作業系統、虛擬機器監視器或其他系統軟體遭破壞的情況下容易受到攻擊。

機密運算採用基於硬體、低於系統軟體層級且不受軟體型攻擊的措施來改善這種隔離。漏洞的減少和在使用資料時保護資料的新能力為這些技術的快速普及奠定了基礎，而這一切才剛剛開始。

機密運算市場規模

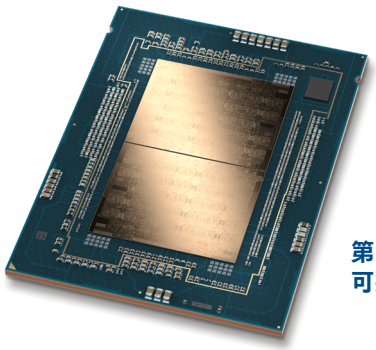
94.4% CAGR
2023-2026[2]

533.1 億美元
到 2026 年[2]

HashiCorp 憑藉其 Vault 祕密資訊管理系統，在推廣和支援企業機密運算方面處於領先地位。Vault 和 Intel® Trust Domain Extensions (Intel® TDX) 的結合，可以使需要機密運算環境來處理敏感工作負載的客戶受益。Intel® TDX 首次在第 5 代 Intel® Xeon® 可擴充處理器中提供廣泛的一般可用性，它在虛擬機器層級隔離 Vault，以在使用時保護祕密資訊：與其他虛擬機器租用戶、虛擬機器監視器、其他系統軟體及管理員隔離。

在效能和工作負載隔離方面處於平台領先地位

第 5 代 Intel® Xeon® 可擴充處理器以獨特的方式，為 HashiCorp Vault 的機密運算提供硬體基礎。除了 Intel® TDX 之外，該平台還提供出色的效能和能源效率。執行資源包括多達 64 個核心（高單核效能），以及用於 AI、加密及其他關鍵工作負載的內建加速器。與第 4 代 Intel® Xeon® 處理器相比，此平衡平台還提供高達 16% 的記憶體頻寬改進[3]和高達 3 倍的最後一層快取記憶體 (LLC)[4]。



第 5 代 Intel® Xeon® 可擴充處理器

該平台包括針對網路安全工作負載進行最佳化的兩個處理器 SKU，專為新一代防火牆、SD-WAN 和 SASE 等工作負載的高處理量、低延遲及高能源效率而設計，也適用於一般雲端運算。

- **Intel® Xeon® Gold 6548N** 處理器（雙插槽、32 核心、2.8 GHz）針對中階安全實作進行調整。
- **Intel® Xeon® Platinum 8571N** 處理器（單插槽、52 核心、2.4 GHz）針對高階安全實作進行調整，並具有高達 3 倍的最後一層快取記憶體 (LLC)。

HashiCorp Vault 和第 5 代 Intel® Xeon® 可擴充處理器的結合，使我們有可能追求新的商業模式。這些模式要求保護共用的敏感資料和智慧財產權，提供有助於實現價值最大化的效能，以及有助於降低營運成本的能源效率。此外，該平台還支援最佳化電源模式 (Optimized Power Mode)，使用者可以在平台 BIOS 中配置該模式，以協助實現特定工作負載下的更佳節能。

機密運算是基於透過解決方案堆疊向上延伸的低階硬體信任根，將敏感或監管資料與特權第三方以及未經授權的軟體和使用者隔離。此信任根實現可信執行環境 (TEE)，並具有消除軟體相依性和相關漏洞的低階硬體基礎。TEE 保護 Vault 及其上執行的操作完整性。與軟體型措施不同，無論權限等級為何，TEE 都會受到保護，防止使用者或軟體未經授權的存取。

第 5 代 Intel® Xeon® 可擴充處理器在前代產品機密運算技術的基礎上得到顯著改進，除了可以相互獨立使用的應用程式層級隔離之外，還具有虛擬機器層級 TEE 的一般可用性。Intel® Trust Domain Extensions (Intel® TDX) 在虛擬機器層級提供隔離和機密性。在 Intel® TDX 機密虛擬機器中，Guest OS 和虛擬機器應用程式會與平台上的雲端主機、虛擬機器監視器及其他虛擬機器加以隔離，以避免存取。它為現有虛擬機器移動到 TEE 提供簡單的遷移路徑，預計 HashiCorp Vault 上的效能開銷將低於 5%[5]。

第 5 代 Intel® Xeon® 可擴充處理器還提供 Intel® Total Memory Encryption (Intel® TME)，作為 Vault 基於 Intel® TDX 實現機密運算實作的技術。Intel® TME 使虛擬機器監視器能夠使用租用戶擁有的唯一加密金鑰，單獨加密多個虛擬機器（或容器）。這種硬體支援的內嵌加密技術不需要變更應用程式，並提供高效能。HashiCorp 和 Intel 的聯合工程已協助 Vault 在新一代機密運算方面引領市場。

祕密資訊與加密管理：HashiCorp Vault

保護應用程式祕密資訊（例如加密金鑰、密碼、權杖、憑證及其他敏感資料）是機密運算的核心目標。HashiCorp Vault 是廣泛採用的祕密資訊管理系統，執行加密、身分驗證及授權服務，以實現祕密資訊的安全儲存、管理、控制及可稽核性。

受保護的資料可以在 Vault 中安全儲存與管理，其中存取和控制受到嚴格限制，並對可稽核治理措施提供強大支援。Vault 提供圖形和命令列介面來存取其內容，以及使用 HTTP API 進行程式存取。在允許存取之前，Vault 會對使用者、電腦及應用程式等用戶端進行驗證、身分驗證和授權，協助保持強大且一致的安全態勢。這些機制對於理解和控制關鍵資料的存取模式至關重要。

Vault 使用用戶端權杖，依據個別用戶端政策規則來管理存取。這些政策規則限制可以存取哪些資源，以及可以對其執行哪些操作。權杖可以手動建立並指派給用戶端，也可以使用軟體服務以自助服務形式產生。Vault 儲存庫可防止其意外暴露，它還處理身分驗證和授權，以實現強大的存取控制。

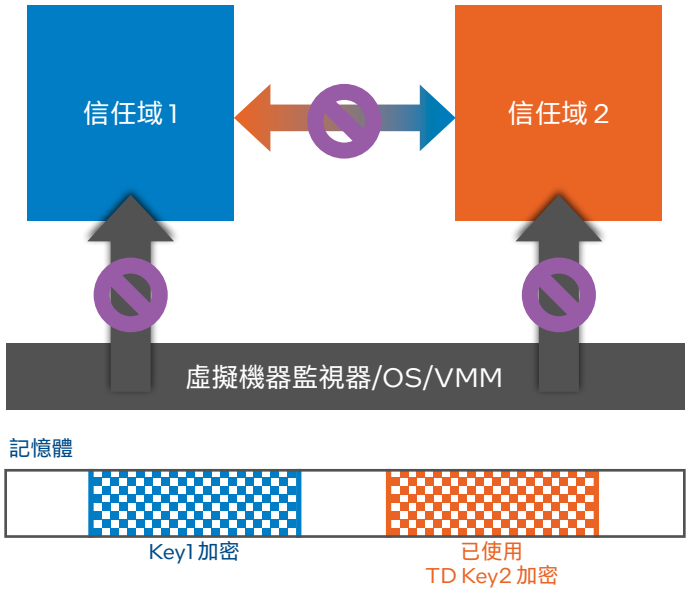
除了保護存取之外，Vault 還提供監控和管理功能，使您能夠瞭解和管理跨平台存取特定祕密資訊的各方、應用程式及服務。Vault 的主要功能包括以下方面：

- **安全的祕密資訊儲存。**Vault 在將祕密金鑰/值對寫入儲存裝置之前對其進行加密，進而在保護儲存裝置本身之外提供額外的保護層。
- **動態祕密資訊。**Vault 可以隨需產生短期祕密資訊，例如資料庫或儲存磁碟區的憑證，並在使用後自動撤銷。
- **即時資料加密。**Vault 可以在不儲存資料的情況下加密和解密資料，使開發者能夠將加密資料儲存在資料庫或其他傳統資料儲存區中，而無須定義加密方案。
- **租賃與續約。**Vault 維護每個祕密資訊的租約，以管理租約到期時祕密資訊的自動撤銷；內建 API 為用戶端提供更新祕密資訊的機制。
- **內建祕密資訊撤銷。**Vault 會自動撤銷一組祕密資訊，例如特定類型的所有祕密資訊或已由特定使用者存取的祕密資訊，這對於金鑰滾動和入侵回應都很有價值。

為了進一步強化祕密資訊的加密隔離，Vault 可以部署在基於 Intel® TDX 的機密運算保護的虛擬機器中。這種方法非常適合 HashiCorp Vault 解決方案的開發，部分原因是它允許現有 Vault 平台適應機密運算，無須變更程式碼，也不影響效能。

使用 Intel® TDX 隔離和保護 Vault

Intel® TDX 透過一種稱為信任域 (TD) 的新型虛擬機器客戶擴展機密運算。每個 TD 都維護自己的保護壁壘，使用透過獨特、專用私有加密金鑰隔離的加密記憶體運作。這種獨立性是深度防禦的關鍵推動因素，可提供基於 Vault 的強化祕密資訊保護，有助於消除企業針對現今高度分散式網路改善安全態勢的障礙，包括實作 ZTNA 和 SASE 等新安全模型。



租用戶使用信任域進行隔離，
每個信任域都使用唯一金鑰進行加密。

由於 Intel® TDX 將整個虛擬機器置於單一信任域內，因此 Vault 可減少對信任邊界之外服務的呼叫。當控制流程超出信任邊界時，與呼叫相關的進入和退出週期均要求硬體執行操作，以保護記憶體和快取記憶體。減少此類操作的需求，是 HashiCorp Vault 基於 Intel® TDX 的機密運算實作提供低開銷和高效能的關鍵。

結論

在第 5 代 Intel® Xeon® 可擴充處理器中， Intel® TDX 的一般可用性為 HashiCorp Vault 提供虛擬機器層級的記憶體保護，無須變更程式碼，也不會造成無法維持的效能影響。隨著應用程式祕密資訊的不斷激增，這種保護將保障網路安全所依賴的身分驗證、加密、授權和存取機制，特別是針對敏感工作負載，包括受 PIPA、GDPR 及 HIPAA 等法規保護的工作負載。HashiCorp 和 Intel 正在進行的聯合工程，將繼續在此基礎上擴展機密運算的未來前景。

進一步瞭解

Intel® Trust Domain Extensions（Intel® TDX）

HashiCorp Vault

解決方案來自：

intel® XEON® + HashiCorp

[1] IBM，「2023 年資料外洩代價報告」（Cost of a Data Breach Report 2023）https://www.ibm.com/reports/data-breach。

[2] Fortune Business Insights，「機密運算市場規模、市佔率及 COVID-19 影響分析」（Confidential Computing Market Size, Share & COVID-19 Impact Analysis）https://www.fortunebusinessinsights.com/confidential-computing-market-107794。

[3] 請於 intel.com/processorclaims 查看 [G12]：第 5 代 Intel® Xeon® 可擴充處理器。結果可能有所差異。

[4] 請於 intel.com/processorclaims 查看 [G11]：第 5 代 Intel® Xeon® 可擴充處理器。結果可能有所差異。

[5] 系統配置：6562C：1 節點、2 個 Intel® Xeon® Gold 6562C 處理器、32 核心、HT 開啟、渦輪開啟、總記憶體 256 GB（16 個插槽/16 GB/4800 MT/s）、1 個適用於 10GBASE-T 的乙太網路控制器 X710、4 個適用於 QSFP 的乙太網路控制器 E810-C 、BIOS American Megatrends International, LLC.3B05.TEL4P1、Ubuntu 22.04 LTS、核心 5.19.17-mvp23v3+6-generic、gcc（GCC）11.4.0、Vault v1.141+ent、dpdk-stable-22.11.1、Vault 基準 v0.1.1、envoy 1.26.2、Open vSwitch 3.2.90、tdx-tools 2023ww22、以 100% CPU 使用率測量的每秒請求數。截至 2023 年 11 月 22 日 Intel 所做的測試。

效能因使用情形、配置及其他因素而異。在效能指數網站進一步瞭解。

效能結果係依配置中所示日期的測試為準，且可能無法反映所有公開可用的更新。請參閱配置備份的詳細資訊。任何產品或元件都無法提供絕對的安全性。

您的成本和成果可能有所差異。

Intel 並不控制或審核第三方的資料。您應該參考其他來源，以評估準確性。

Intel 技術可能需要搭配支援的硬體、軟體或服務啟動。

1123/LH/MESH/353954-001US