SiliconMotion

WHITE PAPER

先進的 FerriSSDs®

因應網路安全性提供完整資料保護的方式

隨著網路擴增、基礎結構和架構的複雜化，我們需要建立更大量和更多類型的連線，然而這些連線很可能成為網路攻擊的目標。

雖然威脅高度複雜化，但是對威脅的感測能力卻相對貧脊，使得追踪大量增長的資訊安全性管控、需求和威脅將變得更為困難。

安全性顯然已是網路安全公司主要關注的課題–必須採取防禦措施，讓硬體免受駭客攻擊或其它未經授權的不當存取，避免資料被竊取或盜用。

慧榮科技的 FerriSSD 磁碟將符合最新企業標準的硬體安全性，與各種額外保護措施相互結合。這些包含了數位簽章韌體和篡改回應，涉及範圍從提出警示到清除磁碟上的所有內容一應俱全。

慧榮科技的 FerriSSD 提供了網路安全性所需的進階安全功能：

保護日常生活的資料

資料中心伺服器、聯網汽車、醫療設備、電競系統，以及工廠控制器、監視系統、零售技術等企業運算服務，只是實現現代生活和工作所需之系統的一小部分。系統記憶體所儲存的資料，可能會揭露與使用者、組織和客戶相關的資訊，如果遭不當利用將可能造成損害。入侵並意圖存取資料的人各有不同動機，例如竊取帳號或信用卡號碼等財務相關資訊、不當揭發機密公司情報或醫療記錄等個人資訊、竊取智慧財產權，以及破壞設備和阻礙運作。

防堵駭客並確保重要資料的安全，是一項需要不時因應變化而調整的挑戰。網路威脅日趨複雜，並且難以預測。現今，隨著「時時連線」之網路連線能力的普及，還有像是聯網汽車等新興應用的行動化，使得硬碟 (HDD) 或固態硬碟 (SSD) 等大容量儲存裝置的系統或使用者資料將更容易受到攻擊。

建置網路安全架構

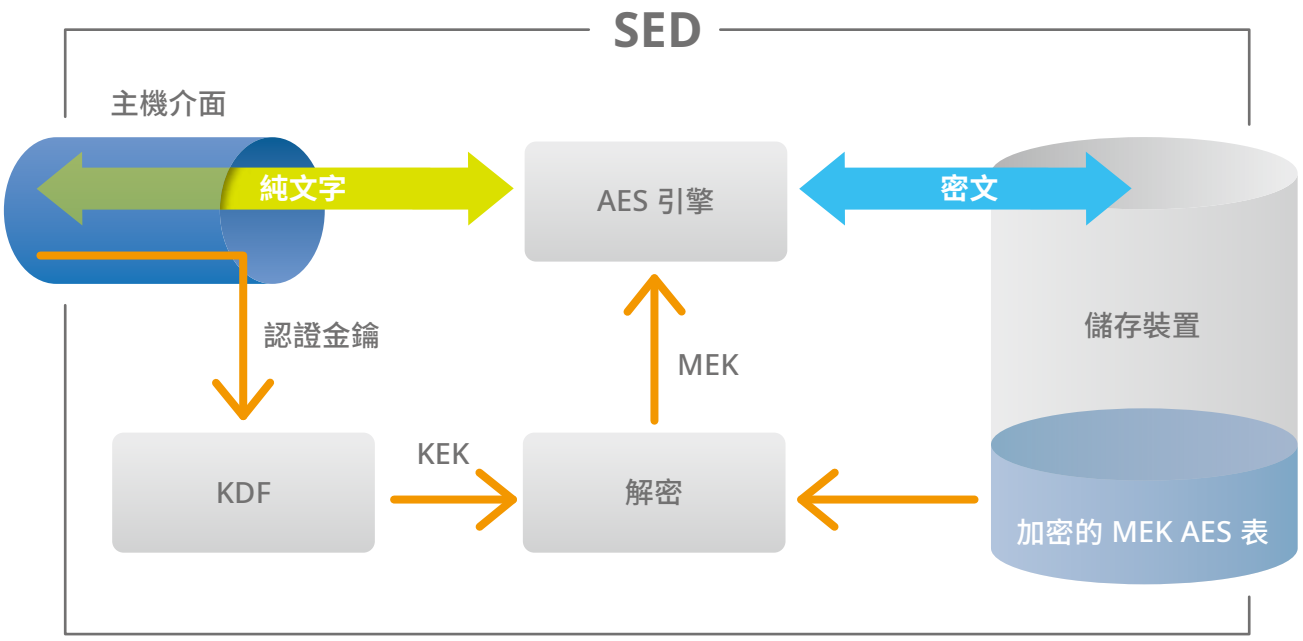
為了防止未經授權的資料存取，並保護資料免受竊取和不當使用，因而需要各種保護措施。為了確保這些保護措施既符合目的又能夠正確實作，企業和監管機構正在建構可將網路安全性置於新產品開發核心的架構。一個實際的範例便是汽車業界的標準：ISO/SAE 21434:2021「道路汽車 — 網路安全工程」。其與聯合國歐洲經濟委員會 (UNECE) 法規 UN 155 密切相關，該法規要求產品開發人員須建立公認的網路安全性管理系統。

ISO/SAE 21434 的範圍涵蓋了從設計到使用年限結束的整個產品生命週期，並包括漏洞分析和保護措施的實施，以確保最全面的網路安全性。此標準評估包括風險評估、辨識和解決網路安全性漏洞，以及測試軟體、硬體元件的應用，以降低風險。車載電子系統規範預計將在 2024-2026 年間強制性標準化。慧榮科技正在與 SGS 合作，以確保所有流程皆符合 ISO 21434 標準，並將在 2023 年第四季前獲得第三方認證。

IntelligentGuard - 加密：防護的最前線

SSD 正逐漸成為大容量儲存裝置的首選。由於沒有主動零件，因此具有無噪音、抗震動、高可靠性、堅固耐用特性，以及低耗電等優點。此外，高效能及快速的系統回應，可縮短資料讀寫時間。使用者通常會將儲存在 SSD上的資料進行加密以保護隱私，以防駭客竊取並對裝置進行破壞或干擾 SSD。傳統的全硬碟加密是由作業系統中的軟體模組來執行。資料是以加密形式從磁碟進行擷取，並經由 PCIe/SATA 介面傳輸後，才在電腦中進行解密。

可支援 AES 256 位元硬體加密技術的自我加密硬碟 (SED) 也是另外一種選擇。自我加密硬碟 (SED) 是一種將加密硬體內建於硬碟控制器的硬碟。SED 會自動加密寫入硬碟的所有資料，並對讀取磁碟中的資料解密。儲存在 SED 的資料一律會使用媒體加密金鑰 (MEK) 進行完整加密保護。MEK 也可以利用使用者指定的驗證金鑰予以加密，藉此鎖定和解鎖 SED。此外，SED 控制也有一些專屬的方法。



不同於傳統由作業系統中軟體模組執行的方法，SED 是採即時加密或解密，所以不會造成主系統 CPU 上的處理負擔。從磁碟中擷取資料時，資料會在 host 端解密，並經由 PCIe/SATA 介面以未加密的方式傳輸到電腦中。在行動和可攜式設備中，更高效率的硬體型加密方法可協助提高能源效率並延長電池壽命。

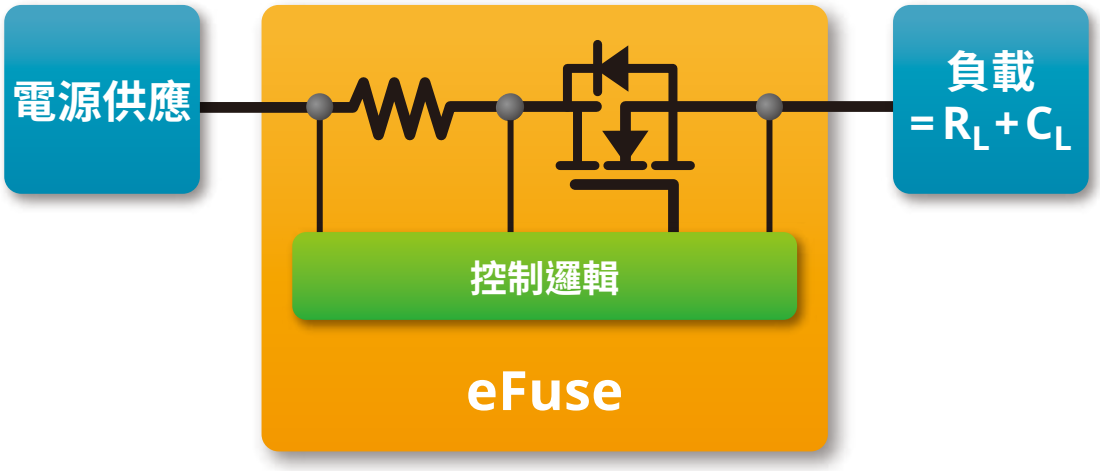
FerriSSD 固態硬碟符合 TCG Opal 2.0 並搭配 AES 256 位元加密。符合此標準能夠協助確保磁碟盡可能安全，防止其遭受未經授權的嘗試來存取儲存在磁碟上的資料。AES 256 位元加密技術是一種業界標準的 256 位元加密演算法，也是業界廣泛使用的加密演算法之一，是美國政府用於機密資訊的加密標準，由於 AES 的加密金鑰是隨機產生的，即使製造商及用戶也無法得知其金鑰密碼，其演算法極端複雜，至今尚未有任何破解。

然而，單方面加密是無法對所有可能的攻擊提供全面性的保護。FerriSSD 還搭配數個資料保護機制，來防範這些不可預期的攻擊風險。針對資料保護與增加儲存裝置可靠度層面，FerriSSD 蘊含多項獨特技術，包含如下。

安全數位簽章驗證機制

其它常見的攻擊包括嘗試藉由載入惡意軟體來奪取 SSD 控制權。此類攻擊像是強制磁碟解密儲存的內容、暴露敏感資料或啟動勒索軟體。為了防止此類攻擊，FerriSSD 產品支援安全數位簽章驗證機制，可在系統啟動時提供安全的數位簽章。利用電子熔絲記憶體 (eFuse)，為 FerriSSD 韌體與軟體加入「電子簽名（Digital Signature）功能；簡言之，eFuse 是一個外人無法碰觸的保護機制，承載一組獨有的密碼金鑰，使得駭客就算入侵 FerriSSD 的韌體，也會礙於無法通過電子簽名驗證程序，因而無法竄改韌體，更無法擅自啟動 SSD。若是驗證簽名失敗，會導致系統向主機處理器傳送安全性警告。

安全數位簽章亦可讓韌體更新以遠端方式套用到 FerriSSD 裝置。



主動式的保護：IntelligentScan™ & DataRefresh™

認證的主動式資料保存，可抵禦物理攻擊

FerriSSD 提供最高 1TB 的儲存容量，採用 16mm x 20mm 表面貼焊 BGA 封裝技術。如此一來，其便可安裝在主裝置外殼內主機處理器附近的板卡或主機板上，相較於傳統的外部 SSD，可確保有更好的保護，以防止物理篡改。

駭客有時會偽裝成緊急的臨時維護來嘗試攻擊目標。透過慧榮獨有的 IntelligentScan 智慧型掃描功能，可依據主機存取行為與工作環境的變化，自動啟動掃描作業，檢測 NAND 記憶體區塊與單元的狀況，並結合 DataRefresh 功能，自動修復或替換存在失效風險的快閃記憶體單元，維持整體儲存裝置的可靠性與穩定性。

此外，FerriSSD 皆支援安全快速清除功能，如果偵測到干擾，便可立即刪除所有資料。還提供了一個臨時斷電保護機制，在發生此類中斷或斷電時，觸發重新整理資料，使用來自板載備用電源的電力，安全地儲存使用者資料。

結論

SSD 固態硬碟提供了節能、小巧和高效能的大容量儲存空間，其強大功能適合各種企業、醫療和汽車運算等應用。為因應防止駭客竊取資料，對於正確地維護儲存之資料的安全性而言至關重要，其加密方式包括在主作業系統中的軟體或嵌入磁碟本身中的硬體進行全磁碟加密。

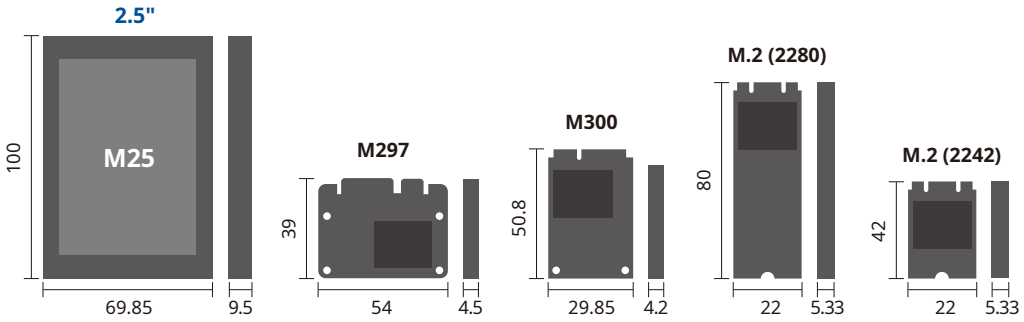
慧榮科技的 FerriSSD 支援硬體型加密技術，其運作時不會增加主系統 CPU 的負載，因此提高了可攜式應用中的效能、能源效率和電池壽命。為了強化和提高加密所提供的保護，進而為現今的網路威脅提供最有效的安全性，FerriSSD 還蘊含多項獨特技術，實現更高等級的資料保護力與可靠度，包括藉由數位簽章、篡改偵測和緊急清除，得以因應發生竊取攻擊時可以進行韌體保護。

FerriSSD® BGA SSD 解決方案

規格	
主機介面	SATA Gen3 PCIe Gen3x2；Gen4 將於 2023 年第 1 季上市
容量	SLCmode：10/20/40/80/160GB；320GB 將於 2023 年第 1 季上市 TLCmode：32/64/120/240/480GB；960GB 將於 2023 年第 1 季上市
外觀尺寸	20mm x 16mm BGA
環保產品	RoHS 相容 / 無鹵素
溫度支援	商用級溫度 (0°C 至 70°C) 工業級溫度 (-40°C 至 85°C)

FerriSSD® 模組解決方案

外觀和尺寸



如需更多 Ferri 家族的相關資訊，請造訪
www.siliconmotion.com 或寄送電子郵件至 **ferri@siliconmotion.com**