DELL Technologies

Microsoft

白皮書

# 結合 Windows Server 2022 和新一代 Dell EMC™ PowerEdge™ 伺服器的功能，獲得進階安全性保護

透過更安全的硬體、韌體和作業系統環境，強化業務關鍵工作負載

Cybersecurity Ventures 指出，2021 年全球網路犯罪估計造成總計 6 兆美元的損失，且到 2025 年將繼續增長至 10.5 兆美元。[1] 光是勒索軟體攻擊，就已在六年內成長了 61 倍，在 2021 年達到 200 億美元，目前每 11 秒就會發生一次攻擊。[1] 2021 年 IDC 調查發現，全球有超過三分之一的受訪組織在過去 12 個月內遭到勒索軟體攻擊或入侵 (而且通常不止一次攻擊)。[2] 雖然 IBM 估計單次資料違規的成本目前為 424 萬美元[3]，但違規事件的真實成本可能遠高於此：在某些情況下，由於勒索軟體攻擊，美國的醫院不得不將急診患者轉至其他醫院並拒絕讓救護車進入。[4]

韌體攻擊對組織來說可能是危害特別嚴重的威脅。這是因為針對韌體的攻擊可能會在作業系統 (OS) (包含作業系統上執行的軟體式安全性) 啟動之前，就植入惡意軟體。然而，只有不到一半的組織採取行動來強化系統以抵禦韌體攻擊，即使針對韌體的攻擊在過去五年內頻率增長了五倍。[5] 工作負載的安全性，畢竟仍取決於其執行所在的整個堆疊。

面對惡意軟體威脅在頻率、種類和成本都呈指數呈長的情況，現代化安全性必須採用多層式做法。這是因為惡意軟體可從硬體和韌體層級或在開機期間入侵系統，凡是僅靠軟體定義型安全性無法抵禦之處，就可能遭入侵。為了克服此漏洞，現代化伺服器的安全性不會是只有單一面向的策略。安全性必須內建在整個基礎結構堆疊中。新一代 Dell EMC™ PowerEdge™ 伺服器與 Windows Server 2022 的組合，可簡化系統管理員協調硬體、韌體及作業系統的重要工作，以充分保護業務關鍵工作負載。

## 結合 Windows Server 2022 安全核心伺服器與新一代 PowerEdge 伺服器的優點

安全核心伺服器是 Windows Server 2022 的新功能，可使用硬體、韌體及作業系統功能，針對當前和未來的威脅提供保護。在新一代 PowerEdge 伺服器硬體上執行 Windows Server 2022 安全核心伺服器軟體，這樣的組合能為像貴公司這樣的組織帶來三大優勢：

- 進階保護
- 預防性防禦
- 簡化安全性

### 進階保護

根據 Microsoft 威脅情報資料，安全核心電腦提供的感染防護是普通電腦的兩倍以上；而現在 Microsoft 透過 Windows Server 2022 安全核心伺服器將此技術帶入伺服器領域。[5] 安全核心伺服器提供的保護，目標在於為伺服器上的關鍵工作負載和資料建立安全的平台。具體來說，安全核心伺服器會使用處理器對動態量測信任根 (DRTM) 技術的支援，將韌體放入硬體式沙箱中。此隔離做法可針對數百萬行高權限韌體程式碼中的漏洞，協助限制其影響。

虛擬化安全性 (VBS) 與 Windows Server 2022 的韌體隔離相輔相成，可將作業系統的關鍵部分 (例如核心程式) 與系統的其他部分隔離開來。這可協助確保伺服器可專注於執行關鍵工作負載，也有助於保護相關應用程式和資料免受攻擊及外流。

為了進一步強化 PowerEdge 伺服器中的韌體，使其免受攻擊，Dell Technologies 會協助維護 PowerEdge 伺服器供應鏈的安全，確保伺服器從工廠運送到客戶地點的過程中，不會遭到篡改 (更詳細的說明請參閱下方的「透過 Dell Technologies 供應鏈完整性提供的額外安全性」)。

## 預防性防禦

安全核心功能有助於主動防禦並中斷攻擊者可能用來惡意探索系統的許多路徑。VBS 中受 Hypervisor 保護的程式碼完整性 (HVCI) 會將程式碼完整性 (CI) 決策功能，與 Windows 作業系統的其他部分隔離開來，這有助於確保核心記憶體僅能透過 CI 驗證，否則無法變為可執行狀態。VBS 也支援使用 Windows Defender Credential Guard，此工具可將用者認證和密碼儲存在虛擬容器中，使作業系統無法直接存取。

受信任平台模組 2.0 (TPM 2.0) 是安全核心伺服器的標準配備，可為敏感金鑰和資料 (例如在開機期間載入元件的測量結果) 提供受保護的儲存區，並能夠驗證在開機期間執行的韌體是否由預期授權單位有效簽署，且未遭篡改，以協助提高安全性。此硬體信任根還能提升 BitLocker Drive Encryption 等功能提供的保護，該功能使用 TPM 2.0，並有助於建立可融入零信任安全策略中的證明式工作流程。同時採用以上多種防禦措施，可讓您的 IT 和 SecOps 團隊可以更妥善地將時間利用在眾多需要注意的安全性領域上。

新一代 PowerEdge 伺服器支援符合業界標準的整合可延伸韌體介面 (UEFI) 安全開機。UEFI 安全開機會檢查在作業系統執行前載入的 UEFI 驅動程式和其他程式碼的密碼編譯簽章，以協助確保惡意軟體並未篡改韌體。此外，PowerEdge 伺服器還支援 TPM 2.0，以提升韌體和作業系統的安全性。

## 簡化安全性

當您購買安全核心 PowerEdge 伺服器時，您可確信 Dell Technologies 提供的整套硬體、韌體和驅動程式均符合安全核心承諾。Microsoft 與 Dell Technologies 密切合作，一同簡化 PowerEdge 伺服器的安全性啟用程序。

Windows Admin Center 中的新功能可讓系統管理員輕鬆配置 Windows Server 2022 安全核心伺服器的作業系統安全功能。全新的 Windows Admin Center 安全性功能可讓系統管理員一鍵啟用進階安全性。Windows Admin Center 會顯示 Windows Server 2022 安全核心伺服器要求的所有安全功能狀態，並讓系統管理員可視需要從單一位置開啟功能。

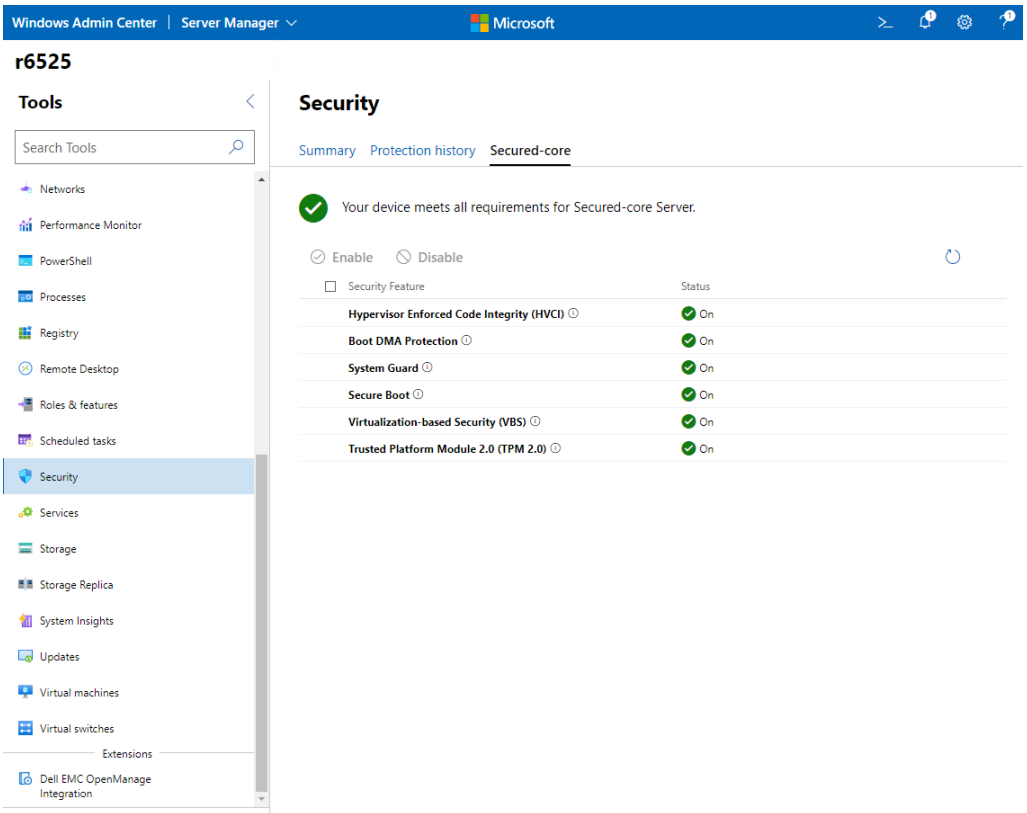



**圖 1**. Windows Admin Center 的安全核心確認畫面

Dell EMC™ OpenManage™ Integration with Windows Admin Center 是 Windows Admin Center 的延伸功能，可進一步簡化安全核心伺服器的管理。這項 Windows Admin Center 延伸功能可透過遠端管理 PowerEdge 伺服器，簡化 IT 系統管理員的安全性工作 (以及其他工作)。在 Windows Server 2022 安全核心伺服器的領域中，OpenManage Integration with Windows Admin Center 延伸功能可讓您在 Windows Admin Center 中檢視您的 PowerEdge 伺服器清查，並提供 PowerEdge 伺服器元件的健全狀況、硬體和韌體清查資訊的整合式檢視。

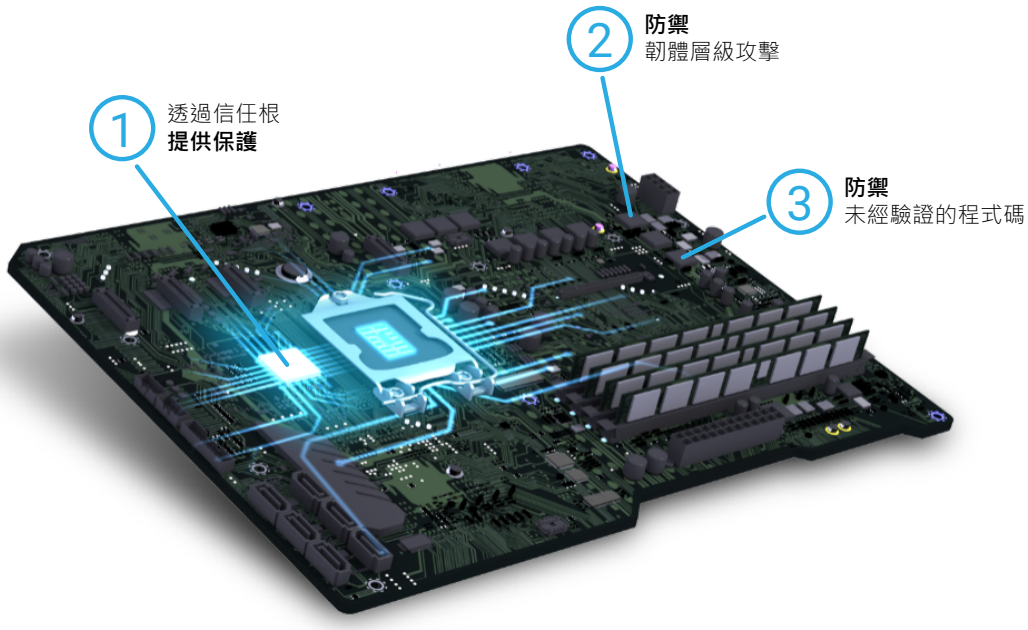
## 適用於 Windows Server 2022 安全核心伺服器的 PowerEdge 伺服器支援

由於安全核心伺服器防禦的多層式性質，因此來自硬體 OEM 的支援至關重要。PowerEdge 伺服器經過 Dell Technologies 的測試和認證，確保硬體和韌體符合 Windows Server 2022 安全功能的要求。此外，PowerEdge 伺服器中的硬體和韌體也已配置為啟用 Windows Server 2022 安全核心伺服器。表 1 詳細說明 PowerEdge 伺服器中的硬體如何為 Windows Server 2022 功能提供基礎。

**表 1**. Windows Server 2022 安全功能及新一代 Dell EMC™ PowerEdge™ 伺服器主要支援功能的對照表

| | Windows Server 2022 | 新一代 Dell EMC™ PowerEdge™ 伺服器 |
|---|---|---|
| 進階保護 | 安全核心系統將韌體置於硬體式沙箱中，以協助限制韌體漏洞的影響。<br><br>VBS 可隔離作業系統的關鍵部分，使其免於進階惡意軟體的侵害。 | Dell Technologies 協助維護 PowerEdge 伺服器供應鏈的安全，確保從工廠運送到客戶地點的過程中，不會發生伺服器遭篡改或韌體遭入侵的情形。 |
| 預防性防禦 | HVCI 和 Windows Defender Credential Guard 等 VBS 功能可防止全類別的漏洞，並能更有效地保護認證等敏感資產。<br><br>TPM 2.0 提供硬體信任根作為安全基礎。 | PowerEdge 伺服器支援符合業界標準的 UEFI 安全開機，可在作業系統執行前，檢查 UEFI 驅動程式和其他程式碼的密碼編譯簽章。<br><br>PowerEdge 伺服器支援 TPM 2.0。 |
| 簡化安全性 | Windows Admin Center 可讓您輕鬆配置安全核心伺服器。 | Microsoft 與 Dell Technologies 攜手合作，一同簡化 PowerEdge 伺服器的安全性啟用程序。Windows Admin Center 與 Dell EMC™ OpenManage™ 的整合功能，可進一步簡化安全核心伺服器的管理作業。 |

## 進階、多層式安全性剖析



## 1 透過信任根提供保護

安全核心伺服器與 Dell Technologies 等領先業界的 OEM 以及 Intel 和 AMD 等晶片廠商合作，使用業界標準硬體信任根，搭配內建於當今現代 CPU 的安全功能。

安全核心伺服器使用 TPM 2.0 和採用 DRTM 的現代 CPU，能以更安全的方式啟動伺服器，並有效減少韌體漏洞。

## 2 防禦韌體層級攻擊

安全核心伺服器使用現代 CPU 中深植於硬體的安全性，將系統啟動至受信任的狀態，防止進階惡意軟體篡改系統及在韌體層級發動攻擊。

System Guard Secure Launch 使用 CPU 驗證裝置，使開機更安全，並有助於防止進階韌體攻擊。

## 3 防禦未經驗證的程式碼

在受信任的運算基礎中執行的程式碼，會在完整狀態下執行，因此不會遭到惡意探索或攻擊。

啟用 HVCI 時，安全核心伺服器只會啟動經由核准的已知授權單位所簽署的可執行檔。Hypervisor 會設定並強制執行權限，以防止惡意軟體嘗試修改記憶體並將其變為可執行狀態。

## 新一代 PowerEdge 伺服器在 Windows Server 2022 中對安全連線的支援

新一代 PowerEdge 伺服器支援 Server Message Block (SMB) AES-256 加密功能，適用於注重安全性的工作負載。這種支援意味著執行 Windows Server 2022 的 PowerEdge 伺服器可為工作負載資料提供端對端加密，以提供額外的安全性。Windows Server 2022 中用於 SMB 的 256 位元 AES 加密相當強大，若使用具適當強度的密碼，甚至足以抵抗量子電腦的暴力攻擊。

PowerEdge 伺服器和 Windows Server 2022 可進一步將端對端 SMB 加密，從個別伺服器延伸至叢集的內部通訊，針對東西向 SMB 資料流使用 AES-256 加密。這些額外的 SMB 加密控制可以進一步強化工作負載，並封閉攻擊路徑。

最後，Windows Server 2022 採用第 3 代 Intel® Xeon® 可擴充處理器中的 Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)，以及 AMD EPYC™ Zen 3 處理器中的 256 位元 (vAES256) 向量化 AES 加密。這些進階處理器的指令集可提升 PowerEdge 伺服器中 AES-256 加密的效能。Dell Technologies 和 Microsoft 運用這些進階安全性技術，確保您可以針對業務關鍵工作負載，同時享有強大的安全性及回應能力，不用在兩者間取捨。

## 透過 Dell Technologies 供應鏈完整性提供的額外安全性

Dell Technologies 供應鏈完整性可保護硬體和韌體元件，避免在製造和運送期間遭到入侵。在硬體完整性方面，Dell Technologies 會盡力確保在將產品運送給客戶之前，不會發生產品遭篡改或混入偽造元件的情形。Dell Technologies 所實施的控管措施包含供應商選擇、採購、生產流程和治理，乃至稽核與測試。生產過程中的材料檢查有助於識別標記錯誤、偏離正常效能參數，或包含錯誤電子識別符的元件。

在軟體完整性方面，除了防止出現任何程式碼漏洞外，Dell Technologies 也力求確保在將產品運送給客戶之前，不會發生韌體或裝置驅動程式遭植入惡意軟體的情形。Dell Technologies 在全球所有生產據點均具有 ISO 9001 認證。嚴格遵守這些程序和控管措施，有助於盡可能降低 Dell Technologies™ 產品遭混入偽造元件，或韌體或裝置驅動程式遭植入惡意軟體的風險。此外，Dell Technologies 會在軟體開發生命週期 (SDLC) 程序中落實這些措施。

Dell Technologies 也會盡力協助確保製造設施和運輸鏈的實體安全。Dell Technologies 要求製造 Dell Technologies 產品的特定工廠必須符合美國運輸資產保護協會 (TAPA) 指定的設施安全要求，包括在關鍵區域使用受監控的閉路攝影機、出入控制，以及持續看守出入口。Dell Technologies 在其領先業界的物流計畫中，也實施了保護措施，防止產品在運輸過程中遭到盜竊和篡改。最後，適用於 PowerEdge 伺服器的 Dell Technologies Secured Component Verification (SCV)，可讓 Dell Technologies 的客戶驗證所收到的 PowerEdge 伺服器確實是原廠製造的伺服器。

## 透過 Windows Server 2022 和新一代 Dell EMC PowerEdge 伺服器更完善的安全性基礎，保護重要的工作負載

工作負載的安全性取決於其執行所在的基礎。惡意軟體和資料違規的威脅在未來只會繼續增加，惡意分子持續探索無法以傳統軟體式安全性防範的攻擊途徑，尤其是一大原因。韌體攻擊會專門針對開機期間的伺服器，甚至在軟體式安全性尚未開始保護系統前，就會發動攻勢。保護現代化伺服器需要跨硬體、韌體和作業系統的多面向安全性。

比起以往，現在更有理由升級至 Windows Server 2022。Windows Server 2022 中的安全核心伺服器功能可協助組織抵禦針對韌體和作業系統的威脅。執行 Windows Server 2022 的新一代 Dell EMC PowerEdge 伺服器搭配 Dell Technologies 的硬體和軟體完整性保護機制時，可為硬體、韌體和作業系統的整個堆疊提供現代化安全性。而新一代 PowerEdge 伺服器也支援 Windows Server 2022 中的安全連線功能，這項功能可將此安全性從個別伺服器延伸至資料中心內的整個叢集。此外，Windows Server 2012 的支援於 2023 年 10 月結束，這表示該現在正是開始制定升級計畫的好時機。[6]

若要進一步瞭解 Windows Server 2022 與新一代 Dell EMC PowerEdge 伺服器可如何協助保護您的關鍵工作負載與資料，請造訪 www.delltechnologies.com/en-us/solutions/microsoft-oem/。

[1] Cybersecurity Ventures. “Cybercrime To Cost The World $10.5 Trillion Annually By 2025.” 2020 年 11 月。 https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.
[2] IDC. “IDC Survey Finds More Than One Third of Organizations Worldwide Have Experienced a Ransomware Attack or Breach.” 2021 年 8 月。
[3] IBM. “How much does a data breach cost?” 2021.www.ibm.com/security/data-breach.
[4] Dan Goodin. “Hospitals hamstrung by ransomware are turning away patients.” *Ars Technica.* 2021 年 8 月。 https://arstechnica.com/gadgets/2021/08/hospitals-hamstrung-by-ransomware-are-turning-away-patients/.
[5] Microsoft. “New Security Signals study shows firmware attacks on the rise; here’s how Microsoft is working to help eliminate this entire class of threats.” 2021 年 3 月。 www.microsoft.com/security/blog/2021/03/30/new-security-signals-study-shows-firmware-attacks-on-the-rise-heres-how-microsoft-is-working-to-help-eliminate-this-entire-class-of-threats/.
[6] 於本文撰寫時。如需 Windows Server 2012 結束支援的相關最新資訊，請造訪 Windows Server 2012 生命週期頁面： https://docs.microsoft.com/en-us/lifecycle/products/windows-server-2012。



DELL Technologies

Microsoft



使用 Windows Server 2022 進行現代化。
支援雲端的作業系統，可透過混合式功能為內部部署投資加值。