DELL Technologies

Dell ThinOS 安全性優勢

無論地點皆可自信地完成工作

採用可增強虛擬桌面和桌面即服務環境安全性的解決方案。

使用 Cloud Client Workspace 軟體和 Dell 精簡型用戶端解決方案，在維持安全性的情況下滿足不斷演變的員工需求並提高效率。

Dell 精簡型用戶端解決方案是經過最佳化的 VDI 端點，旨在透過現代化 IT 管理，讓您能夠安全且順暢地存取虛擬桌面與桌面即服務環境。

使用 Dell 獨家的 ThinOS 盡可能地減少攻擊面，讓您高枕無憂，ThinOS 是我們專為虛擬工作空間打造的最安全精簡型用戶端作業系統[1]。

深入瞭解產品組合 ->

Dell ThinOS：支援零信任

透過 Dell ThinOS 和 Wyse Management Suite 強化零信任策略

隨著網路威脅不斷演進，組織將採用零信任安全性模型來防範資料違規事件。Dell Technologies 透過 Dell ThinOS 和 Wyse Management Suite (WMS)，提供安全、可管理且原則導向的解決方案，協助 IT 領導者強化虛擬環境中的端點安全性。

不信任任何裝置

在零信任模型中，即使是 ThinOS 裝置也不應自動受到信任。Wyse Management Suite (WMS) 將新用戶端置於預設原則群組以實現安全上線，需要先取得管理員核准再套用組態。透過 WMS 或 SCEP 伺服器管理憑證的 802.1x 或 EAP-TLS 等安全連線，可提供強化保護。其他措施，包括限制帳戶權限、設定唯一 BIOS 密碼，以及使用裝置安全性拒絕清單，皆可進一步降低安全性風險。

不信任任何應用程式

在裝置模式中，Dell ThinOS 的設計搭配無殼層存取權、AES 加密分割區和安全開機，可確保安全的應用程式支援，藉此防止竄改。只有 Dell 核准的應用程式套件可透過 WMS over SSL 部署，並使用雜湊和簽名驗證來偵測損毀或未經授權的變更。管理員可以通過僅部署必要的軟體元件、將選用商用瀏覽器使用限制在必要工作流程、將暴露風險降至最低，並增強應用程式層級安全性來降低風險。

不信任任何使用者

ThinOS 環境中的使用者存取受到嚴格管理，以符合零信任原則。虛擬代理程式驗證可確保使用者只能存取指派給他們的桌面或應用程式。多因素驗證新增了關鍵的身分識別保護層，同時與 Imprivata OneSign 或 Identity Automation 等平台整合，以強化工作階段控制。這些綜合措施有助於阻止未經授權的存取，並協助符合企業安全性標準。

專為安全而精心設計

保護使用者裝置

保護本機資料

安全存取 VDI 工作階段

安全設計

Dell ThinOS 作業系統是以安全性為核心目標所專門打造的。這套解決方案採用以裝置為基礎的設計，擁有封閉式架構，有助於盡可能減少漏洞。只有經過 Dell 嚴格測試、封裝和認證的第三方應用程式和驅動程式可以進行安裝，這一點確保為您的關鍵任務作業提供受控且安全的環境。

安全儲存裝置

在裝置模式下運作時，沒有命令殼層，也無法遠端檢視、變更或刪除用戶端上儲存的作業系統、應用程式或組態檔。透過安全開機和 AES 裝置特定快閃記憶體加密進一步增強安全性，為關鍵元件提供健全的保護。

強化攻擊面

結合安全映像建立和儲存與不對外公開的 API，Dell ThinOS 打造了一個經過強化的攻擊面，可抵禦常常侵擾 Windows 和 Linux 裝置的病毒和惡意軟體。

防止常見漏洞

Dell ThinOS 的設計著眼於安全性。為了完善地防範常見的安全性威脅，它可以流暢連線到虛擬環境，無須商用瀏覽器。對於有進階需求的客戶，它提供進行安裝的選項。

安全性管理

保護使用者裝置

保護本機資料

安全存取 VDI 工作階段

BIOS 和 CMOS 安全性

使用 Dell 用戶端裝置時，ThinOS 可讓您輕鬆遠端保護 BIOS。只需按幾下，就可以使用 Wyse Management Suite Pro 版本在多個裝置上大規模部署 BIOS 升級和設定，例如 BIOS 密碼。

自動化憑證管理

使用 Wyse Management Suite 可輕鬆部署全域憑證。此外，ThinOS 還支援簡易憑證註冊協定 (SCEP)，簡化了唯一裝置憑證的管理。

安全連線

Wyse Management Suite 可以在公開和私人網路上使用安全、加密的 HTTPS 連線，安全地管理和升級 ThinOS 裝置。

安全映像建立

ThinOS 映像專為安裝在特定的 Dell 用戶端裝置上而打造，可確保最佳相容性和效能。為了防止篡改，這些映像在透過 Wyse Management Suite 或 Dell OS Recovery Tool 部署時，會納入進階安全性措施。

主要保護措施包括：

- 使用檢查總和驗證以驗證資料完整性
- 使用數位簽名驗證以驗證映像來源
- 使用唯一平台金鑰，確保與用戶端硬體和預先安裝作業系統的相容性

安全通訊

保護使用者裝置

保護本機資料

安全存取 VDI 工作階段

SSL 連線

所有代理程式和通訊協定通訊都可以透過安全連線完成。通訊原則可以在全域或個別層級定義 ThinOS，以實施所需的安全性層級。三個「受支援」層級分別是：

- 高 – 要求憑證驗證
- 警告 – 如果憑證驗證檢查失敗，則需要使用者接受
- 低 – 不要求憑證驗證

有線和無線安全性

所有有線和無線 802.1x 企業通訊都可以使用 WPA/WPA2 PSK/Enterprise 搭配 EAP-PEAP、EAP-LEAP、EAP-TLS 或 EAP-FAST 進行保護。

代理程式通訊協定安全性

與 Windows 和 Linux 桌面一樣，ThinOS 在使用 RDP、HDX、BLAST、DCV 和 PCoIP 通訊協定連結虛擬環境代理程式和伺服器時，會啟用加密和壓縮功能。此外，ThinOS 還支援 FIPS 140-2，可確保在機密環境中進行安全通訊。

本機使用者安全性

保護終端使用者資料並控制本機使用者存取

保護使用者裝置

保護本機資料

安全存取 VDI 工作階段

篡改防護

ThinOS 權限設定透過限制使用者對桌面功能表的存取來提供健全的桌面安全性，防止未經授權的檢視或變更。IT 管理員擁有完整的使用者介面存取權，可確保完整的控制和簡化的作業。此外，ThinOS 還可連線到虛擬環境，無須安裝本機瀏覽器。

安全終端使用者認證

在預設情況下，ThinOS 裝置只會將 SignOn 認證和應用程式快取物件 (例如工作階段點陣圖) 儲存在 RAM 中，直到工作階段結束。SignOn 認證或通訊協定物件不會寫入裝置的快閃記憶體檔案系統。對比之下，Windows 型和 Linux 型裝置通常使用磁碟快取來保留認證和應用程式快取，這使得它們更容易受到資料違規或駭客入侵的影響。

進階驗證和權杖

支援採用 CAC 和 PIV 智慧卡搭配 90Meter 和 ActiveIdentity 中介軟體，以及採用 Yubikey 裝置搭配 FIDO2 的權杖型驗證。

USB 和本機磁碟安全性

儲存在用戶端本機快閃記憶體檔案系統上的所有 ThinOS 映像系統檔案、套裝檔案、快取組態和鏡像儲存庫物件都經過 AES 加密，以盡可能降低資料洩露的風險。

若為配備受信任平台模組 (TPM) 的裝置，部分雜湊金鑰儲存在此元件中。因此，即使從裝置中移除快閃記憶體模組，這些模組上的資料仍然無法存取。此外，用於建立安全 SSL 連線的憑證一旦載入並儲存在裝置的快閃記憶體中，就無法匯出。

- **所有快取的目的地均為 RAM，且皆屬於非持續性性質**
- **系統會將 AES 加密套用在所有分割區/檔案**
- **重設為原廠預設值會將裝置還原成出廠時的組態狀態**
- **裝置特定快閃記憶體加密和安全開機**

Dell ThinOS 可讓您精確控制 USB 大容量儲存裝置。您可以定義哪些使用者具有存取權，以及他們使用這些裝置的方式，同時確保安全性和彈性。

1 Flexible controls for IT support

管理權限可用於控制用戶端故障排除。用戶端紀錄可以匯出到 WMS 或本機 USB 金鑰。

系統會將用戶端裝置組態儲存到安全的非 OS 快閃記憶體分割區。您可以使用重設為原廠預設值來清除這些組態。

系統會將用戶端憑證和映像檔案儲存在安全的非 OS 儲存分割區。您可以使用重設為原廠預設值來清除這些憑證。

2 USB 大量儲存虛擬環境存取權的彈性控制

ThinOS BIOS

您可以在裝置以本機方式或透過 Wyse Management Suite 控制台，藉由 BIOS 組態來啟用/停用 USB 連接埠。停用 USB 連接埠適用於所有 USB 裝置類別。

隱私權與安全性

裝置安全性會根據 VID/PID 或 USB 類別來允許或拒絕對 USB 裝置的存取。它允許選擇性限制對任何連接到 ThinOS 用戶端裝置之裝置的存取。

週邊設備

USB 重新導向設定可用來強制 USB 裝置驅動程式支援來自虛擬主機，而非 ThinOS 用戶端裝置。

工作階段設定

全域和供應商特定的合作夥伴原則可用於控制 USB 裝置對應和重新導向。

最安全之搭載 Dell ThinOS 的精簡型用戶端[1]

從第一次開機就安全無虞

Dell 專屬精簡型用戶端作業系統專為安全而精心設計，可以盡可能降低風險並保護虛擬桌面和桌面即服務工作階段。

受信任的端點

支援熱門認證方法、法規遵循標準和非持續性的資訊，以保護工作階段資料與充滿信心隨處連線。

安全性管理

Wyse Management Suite 的精細集中式控制有助於強制執行安全性原則、設定裝置法規遵循設定和管理 BIOS。

封閉式架構

本機裝置上不會公開任何敏感性資料或個人資訊。透過系統強化來限制攻擊面、未發行 API、資料加密，以及 Dell 獨立封裝的檔案，可以防範病毒與惡意軟體。

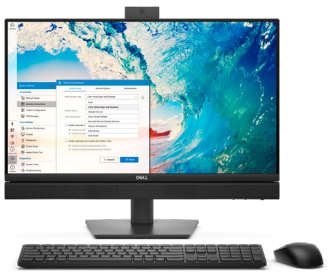
安全終端使用者認證

將使用者認證儲存在 RAM 中有助於保護其免受惡意軟體的侵害，以及在重新啟動時進行清除，降低未經授權存取的風險。

安全通訊

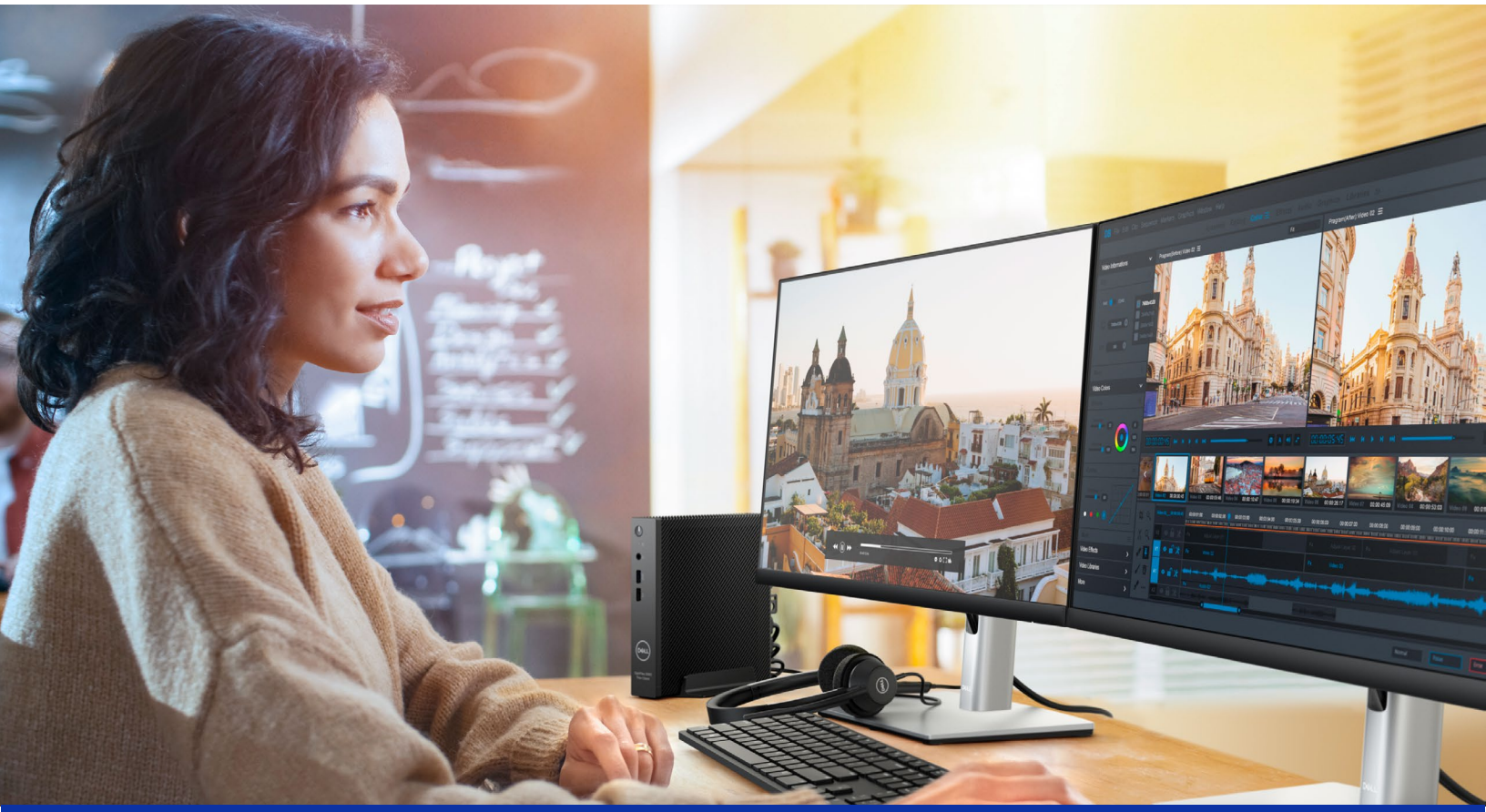
ThinOS 支援所有代理程式通訊協定的 SSL 連接，並支援用於安全有線和無線企業網路存取的進階加密方法，藉此確保安全的通訊。

OptiPlex 3000 精簡型用戶端 - >



Dell Pro 多合一電腦 35 W - >

Dell Pro 14 筆記型電腦 - >



使用 Dell ThinOS 和 Dell 精簡型用戶端解決方案，隨時隨地放心工作

經過最佳化且安全的 VDI 端點，適用於您的虛擬桌面基礎結構和桌面即服務解決方案。

期待與您相見
dell.com/CloudClientWorkspace

瞭解詳情
簡化 IT 部落格 -->

加入對話
LinkedIn / X

資料來源與免責聲明

[1]根據 Dell 在 2025 年 1 月對裝置模式下肢 Dell ThinOS 與競爭產品所做的分析。

[2]Dell ThinOS 裝置模式是 Dell ThinOS 的預設運作狀態，其設計可從最初就強制執行穩健的安全性狀態。在版本 2508 及更新版本中，ThinOS 可為 IT 管理員提供更大的彈性，藉此允許安裝商用瀏覽器選項和部署第三方軟體元件。為確保與 ThinOS 10 相容，第三方應用程式必須與 Ubuntu 24.04 x86_64 相容 (包含 Debian 安裝套裝)，並成功通過應用程式建置器工具中的所有作業系統相依性檢查 (視用戶端裝置的功能而定)。部署需要在隔離模式或原生模式之間做出選擇。在原生模式下運行的應用程式可能會基於其作業行為受到限制。強烈建議您在部署前先進行全面測試，以確認安裝成功且功能正常。如需受支援應用程式和部署指南的完整詳細資料，請參閱 Dell.com/support 上的客戶安裝指南。