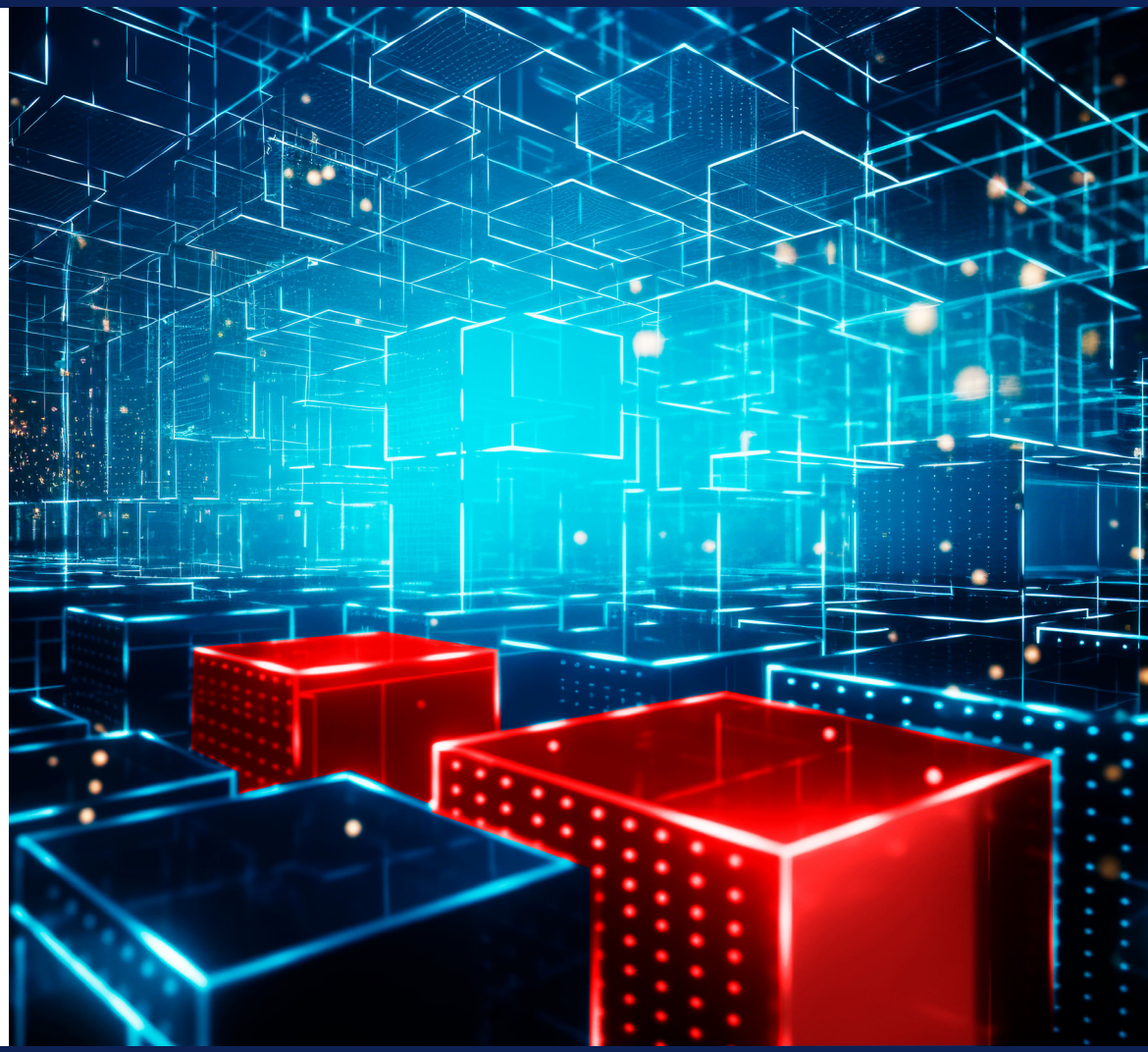
如何保護端點 AI 的使用

以安全的現代化裝置和攻擊者思維來保護裝置上 AI (人工智慧) 工作負載。



執行摘要

裝置上 AI 擁有巨大效益，但也伴隨網路風險。在本電子書中，我們將逐步解說如何讓貴組織安全享有優勢，以善用端點的 AI 創新。

目錄

裝置上 AI 的攻擊面

可能受到攻擊的目標

所有新興技術都伴隨網路安全性風險，原因只有一個：這是全新的領域。您面臨的是未知事物。我們已在雲端運算、區塊鏈和許多其他技術中見過這種情況。裝置上 AI 也面臨同樣的狀況。一如既往，緩解這種風險的關鍵就是去瞭解未知領域。

開始談論需要哪種安全性來盡可能減少攻擊面之前，先談論我們保護的目標和原因會比較有幫助。請把網路環境想像成是一棟商業大樓中的管線系統，這棟商業大樓有多家企業進駐。這些管線在整棟大樓中，為各式各樣的使用案例運送自來水、天然氣等資源。如果流經管線的物質遭到汙染或中斷，就無法發揮作用。如果運送物質的管線受損或損毀，就無法進行運送。管線及內容物都必須處於良好運作狀態，才能滿足各自使用案例的需求。▶

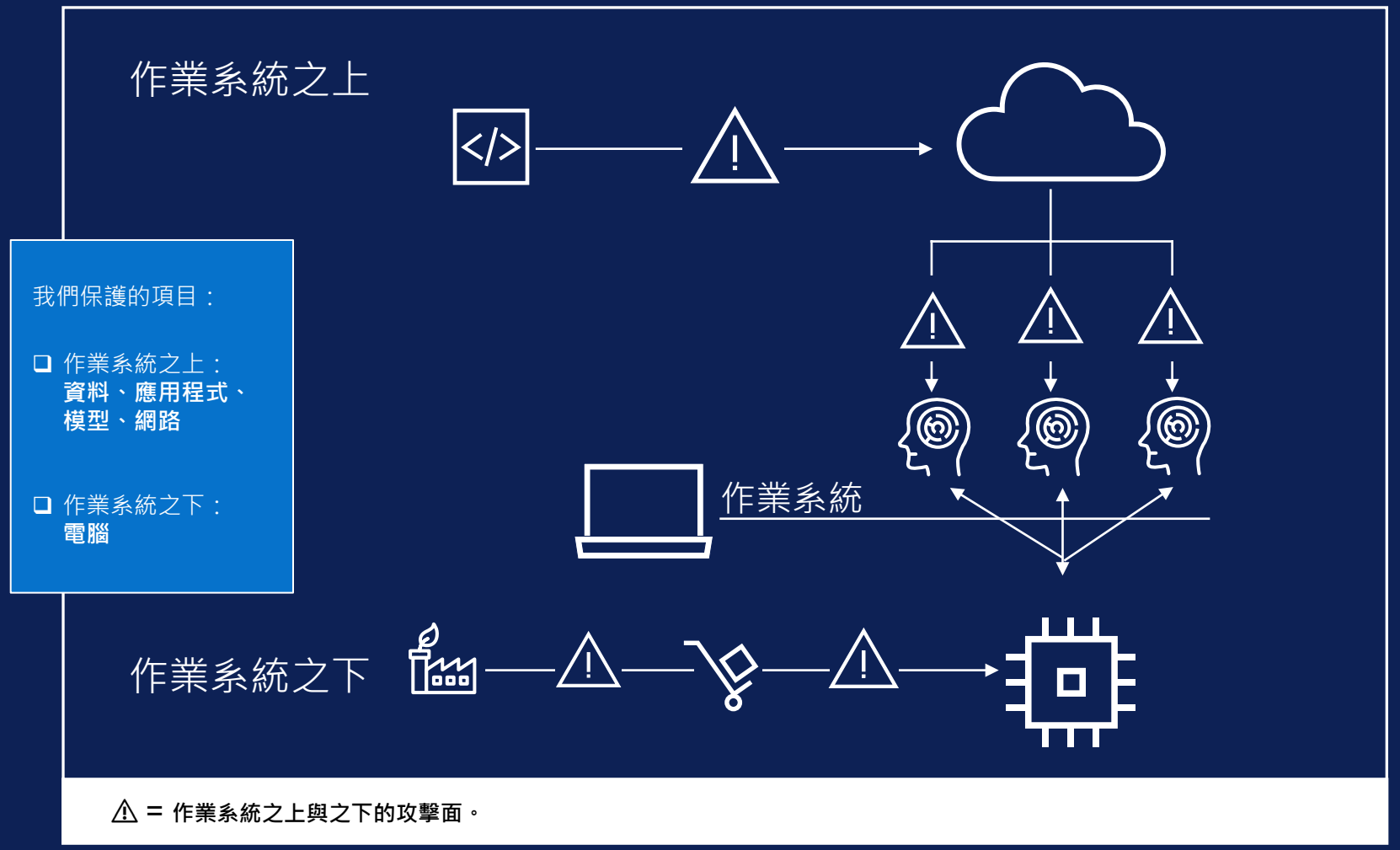
裝置上 AI 的攻擊面 (續)

可能受到攻擊的目標 (續)

回頭來談端點 AI：

- 管線就是基礎結構，即電腦和企業網路。也就是工作的工具和地點。
- 流經管線的內容物就是驅動各種 AI 使用案例的資料、應用程式和模型。也就是執行工作所需的資產和資源。

您猜得沒錯。兩者都是網路罪犯會鎖定的目標。他們可能會竊取用於勒索的 IP，或是破壞資料或模型來影響營運。無論如何，後果都可能十分嚴重，會造成財務和聲譽損害及/或導致監管審查。▶



端點的安全性風險

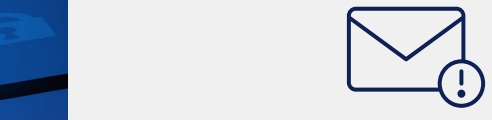
攻擊者的入侵手法

接下來討論攻擊者可能用來存取這兩種目標的方法。

裝置入侵。正如《Endpoint Security Market Insights》(端點安全性市場深入解析，Forrester Research, Inc.，2025 年 3 月) 中所述，電腦是現代網路威脅的其中一種主要目標。這類攻擊的發生時間可能會比裝置上 AI 開始運作的時間還要早很多，也就是說，這類攻擊屬於**硬體或軟體供應鏈攻擊**。在供應鏈期間有數十甚至數百個時間點，可讓惡意人士竄改元件 (如電路、韌體) 以導入弱點，供後續惡意探索利用。想像一下，一家投資公司要是收到一批裝有偽造元件的全新電腦，將會面臨什麼災難。

身分洩露。涉及失竊或外洩認證的入侵是成長最快的攻擊手法之一。這點不足為奇。使用有效認證的攻擊者可登入電腦，在企業網路中來去自如，而且長期不被發現。IBM 最新的 Cost of a Data Breach report (資料違規損失報告) 顯示，這些入侵行為平均要過 292 天才會受到識別並遏阻，是所有經研究攻擊手法中持續最久的。對威脅發動者而言，這種層級的存取權價值高到難以忽視。事實上，Zscaler 的研究顯示，惡意人士正在升級認證竊取計謀，打算利用 GenAI 來改進和擴大網路釣魚攻擊。這種套用到機密訓練或推論資料，或是直接套用到模型的未授權存取，都可以歸類為**模型供應鏈攻擊**。

內部威脅。近期研究顯示，相較於其他攻擊手法，**惡意內部攻擊**所導致的損失最高，平均為 499 萬美元。請記住，內部攻擊可能會發生在硬體供應鏈、軟體供應鏈和模型供應鏈中。▶



終端使用者因**網路釣魚**電子郵件而上當的中位數時間：<60 秒*

平均要花 292 天才能發現並遏阻**認證洩露****

惡意內部攻擊造成平均 499 萬美元的損失**

**資料來源：《Verizon DBIR》，2024 年*
資料來源：《IBM Cost of a Data Breach Report》(IBM 資料外洩損失報告)，2024 年

應備妥的防範措施

什麼措施可緩解風險

這些攻擊目標都不是全新的概念。攻擊者的最終目標也都是老生常談。一如既往，我們要聚焦在保護機隊和使其具備復原能力。**防範措施分層**有助於立即減少攻擊面並探明任何可疑行為。

零信任思維可緩解整個機隊的風險。這些原則 (絕不信任、一律驗證和持續監控) 可協助您永遠領先攻擊者。要封鎖所有攻擊是不可能的。若要擁有強大的安全性狀態，就需要對整個 IT 生態系統擁有**可見度和控管機制**。

請將這個架構納入考量，重新評估您的基礎結構，尤其是會與 AI 互動的系統和程序。哪些防範措施可盡量減少裝置入侵、身分洩露和內部威脅的風險呢？▶

零信任原則有助於抵禦風險並縮短網路活動災難影響範圍

應備妥的防範措施 (續)

什麼措施可緩解風險 (續)

整體防範措施分為兩個類別。

「作業系統之下」安全性可保護您使用的 AI 裝置。
我們可將這點分成兩個部分：

- 透過**安全打造**的裝置來保護機隊。這表示使用安全設計的 AI PC (也就是採用安全設計原則並在安全供應鏈開發的產品)。
- 透過**內建安全性**的裝置來保護機隊。安全的 AI PC 在出廠時即已包含多層提供可見度的嵌入式防護機制，就連 BIOS 和晶片層也包括在內。

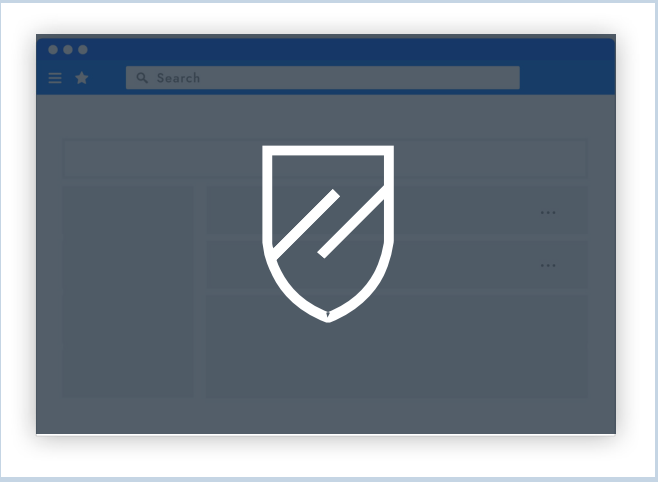
「作業系統之上」安全性可保護 AI 模型的存取權。
透過**軟體安全性**來保護您*處理*的資料和模型，以及您*在*其中工作的企業網路。必須保護機器學習安全性作業，以及監控已部署 AI 工作負載的網路流量。▶

作業系統底層安全性

安全的 AI PC

硬體和韌體安全性、供應鏈安全性、核心晶片

作業系統上層安全性



軟體安全性

為端點、網路與雲端環境提供額外一層安全性

可整合所有要素的安全性服務和專業知識。

為機隊套用最佳實務

Dell AI PC 如何為機隊提供基礎安全性

這正是 Dell Trusted Workspace 發揮作用的部分。我們的技術專家深刻瞭解攻擊者思維，並以此策劃和設計我們商用 AI PC 的安全性。

作業系統之下、安全的設計、強大的供應鏈控管和選購的供應鏈保證，均有助於確保電腦從第一次開機起就安全無虞。內建的硬體和韌體安全性可在使用電腦時持續保護電腦，例如 Dell 獨家* BIOS 層級竄改偵測 (Dell SafeBIOS)，以及可抵禦未授權存取的無密碼認證安全性 (Dell SafeID)。不僅如此，Intel® 晶片技術還能協助提供基礎，在 AI PC 用戶端使用 AI 時提供各種層面的防護。例如，Intel 會透過加速磁碟上模型加密，來協助保護用戶端上的待用 AI 資料。►

為機隊套用最佳實務 (續)

Dell AI PC 如何為機隊提供基礎安全性 (續)

若要增強此作業系統之下安全性，可在原廠嵌入我們合作夥伴的 Absolute’ s Persistence 技術，為整個電腦生命週期提供更高的可見度和控管機制，例如在途中為裝置啟用地理位置等功能，以及在最糟情境自行修復重要應用程式。

事實上，Dell 已策劃出軟體合作夥伴生態系統解決方案，包括 CrowdStrike Falcon XDR 和 Absolute Secure Access，這兩者可啟動零信任原則，以保護模型供應鏈免於**作業系統之上**的未授權存取。運用這些解決方案，您可以建立和強制執行具有精細存取控制 (例如，角色型存取控制，簡稱 RBAC) 的原則，以緩解惡意內部存取或 AI 模型竄改的風險。►

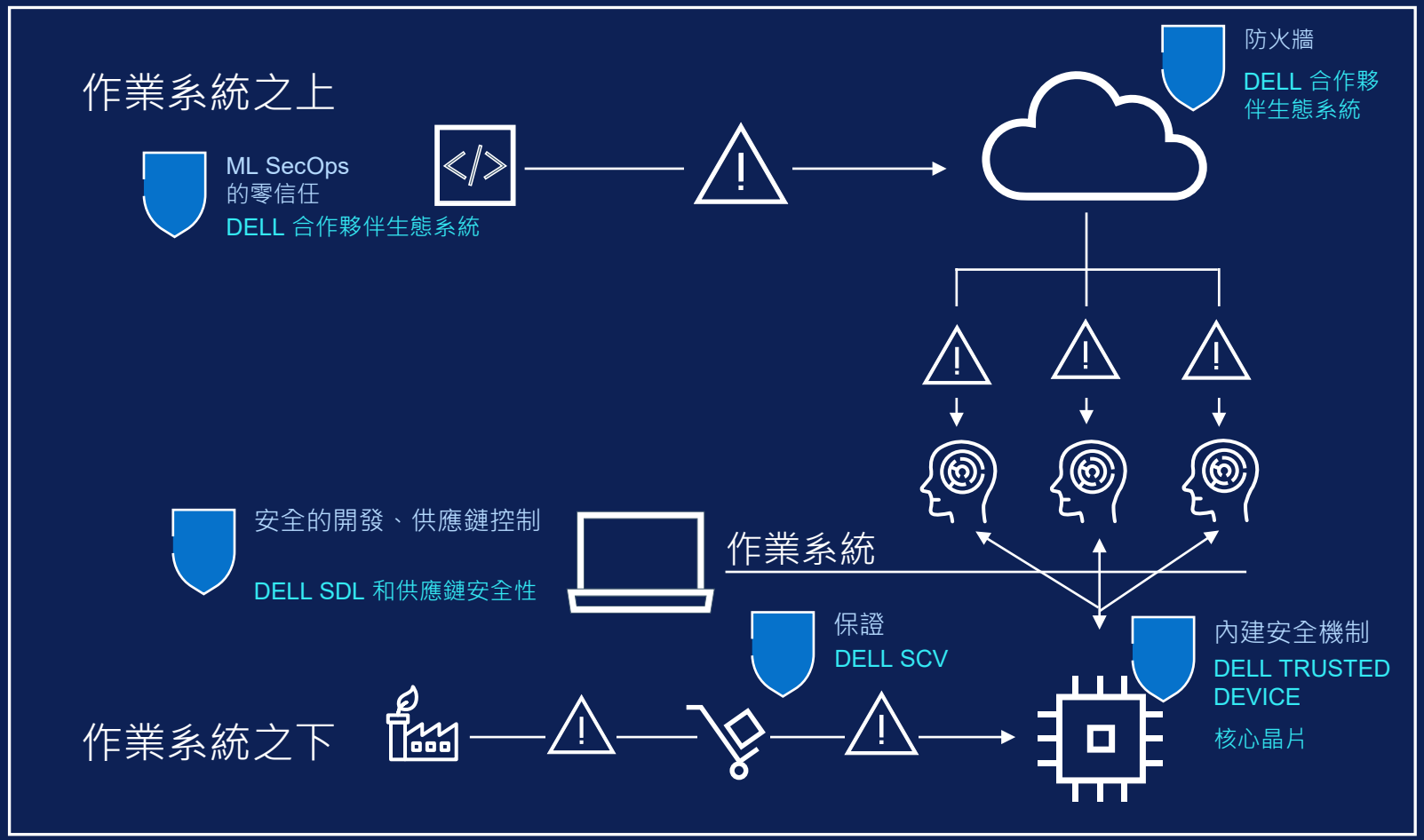
為機隊套用最佳實務 (續)

Dell AI PC 如何為機隊提供基礎安全性 (續)

這些措施統稱為 ***AI 安全性***。這些功能可保護裝置上 AI 工作負載免受網路攻擊，讓您能夠持續專注在創新和贏得業務。▶

透過協調軟體與硬體防禦來阻止進階端點攻擊

Dell 與 Intel 及 CrowdStrike 合作，將作業系統之下及作業系統之上層級與硬體輔助安全性整合起來。
深入瞭解 >



主要重點與後續步驟

透過 Dell 技術保護端點 AI

企業對 AI 充滿期待，但 Absolute 對 CISO 進行的近期問卷調查顯示 AI 整備度有所落後。對數百萬部裝置的分析結果顯示，電腦族群無法廣泛接受新的 AI 功能。**Dell 可協助您整合所有功能。**

根據安全的現代化基礎來開發和部署 AI 模型。 Windows 10 支援於 2025 年 10 月終止。電腦將再也無法接收安全性更新、功能更新和 Windows 10 支援。舊型裝置可能會不符合 Windows 11 要求，而且可能會缺少最新的內建效能、安全性和 AI 增強功能。升級到搭載具備 Intel vPro® 之 Intel® Core™ Ultra 處理器的 **Dell Pro** 或 **Dell Pro Max**，可透過**全球最安全的商用 AI PC** 來發揮安全性效益和保護 AI 工作負載。*►

Windows 10 支援將於 10 月終止。

升級至搭載 Intel 技術的最新 Dell AI PC，發揮安全性效益和 AI 增強功能：

選購 Dell Pro ● Dell Pro Max

*全球最安全的商用 AI PC**

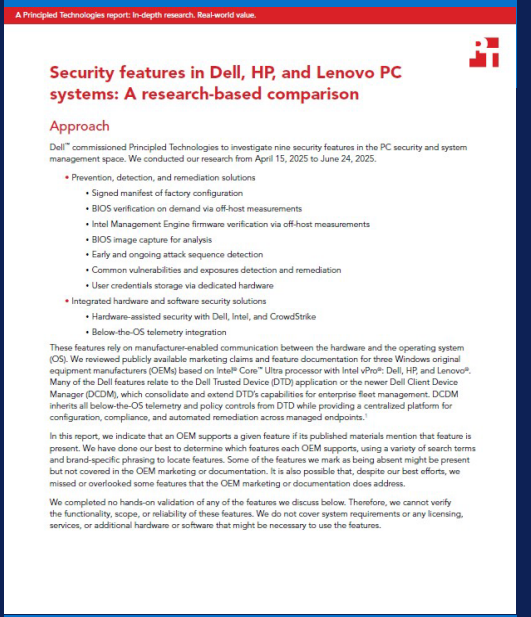
探索改善安全性狀態的加值軟體和服務：

軟體與整合

服務

業界領導地位

Principled Technologies 發現，Dell 與 Intel 商用 AI PC 安全性優於同業產品


A Principled Technologies report: In-depth research. Real-world value.

Security features in Dell, HP, and Lenovo PC systems: A research-based comparison

Approach

Dell™ commissioned Principled Technologies to investigate nine security features in the PC security and system management space. We conducted our research from April 15, 2025 to June 24, 2025.

- Prevention, detection, and remediation solutions
  - Signed manifest of factory configuration
  - BIOS verification on demand via off-host measurements
  - Intel Management Engine firmware verification via off-host measurements
  - BIOS image capture for analysis
  - Early and ongoing attack sequence detection
  - Common vulnerabilities and exposures detection and remediation
  - User credentials storage via dedicated hardware
- Integrated hardware and software security solutions
  - Hardware-assisted security with Dell, Intel, and CrowdStrike
  - Below-the-OS telemetry integration

These features rely on manufacturer-enabled communication between the hardware and the operating system (OS). We reviewed publicly available marketing claims and feature documentation for three Windows original equipment manufacturers (OEMs) based on Intel® Core™ Ultra processor with Intel vPro®: Dell, HP, and Lenovo®. Many of the Dell features relate to the Dell Trusted Device (DTD) application or the newer Dell Client Device Manager (DCDM), which consolidate and extend DTD's capabilities for enterprise fleet management. DCDM inherits all below-the-OS telemetry and policy controls from DTD while providing a centralized platform for configuration, compliance, and automated remediation across managed endpoints.[1]

In this report, we indicate that an OEM supports a given feature if its published materials mention that feature is present. We have done our best to determine which features each OEM supports, using a variety of search terms and brand-specific phrasing to locate features. Some of the features we mark as being absent might be present but not covered in the OEM marketing or documentation. It is also possible that, despite our best efforts, we missed or overlooked some features that the OEM marketing or documentation does address.

We completed no hands-on validation of any of the features we discuss below. Therefore, we cannot verify the functionality, scope, or reliability of these features. We do not cover system requirements or any licensing, services, or additional hardware or software that might be necessary to use the features.

閱讀研究

免責聲明

*根據 2025 年 7 月由 Principled Technologies 進行的第三方分析，比較搭載 Intel 處理器的 Dell 商用 AI PC 與 HP 和 Lenovo。根據 Dell 於 2024 年 10 月對全球電腦市場進行的內部分析。適用於搭載 Intel 處理器的個人電腦。並非所有電腦均可使用所有功能。部分功能為選購。

深入瞭解：

聯絡我們：Global.Security.Sales@Dell.com

請造訪：Dell.com/Endpoint-Security

追蹤我們：LinkedIn @DellTechnologies | X @DellTech

關於 Dell 端點安全性

不論組織規模大小，安全性都是令人頭疼的議題。**僱用經驗豐富的安全性與技術合作夥伴，實現端點安全現代化。**

Dell Trusted Workspace 可協助確保端點安全，讓您打造支援零信任的現代化 IT 環境。Dell 獨家提供全方位的軟硬體保護產品組合，有助於減少攻擊面和改善網路韌性。我們高度整合的防禦型措施結合了內建防禦和持續警戒，可有效消除威脅。透過為現今雲端型世界打造的安全性解決方案，使用者可保持生產力，IT 團隊也能夠高枕無憂。