探索

Dell Trusted Workspace

隨時隨地為您提供安全防護

使用專為現代雲端環境打造的硬體與軟體防護。

混合式工作模式使組織面臨新的攻擊媒介。隨著對手使用的技術日益複雜，當今的有效端點安全性必須具備多層防禦，以保護裝置、網路和雲端。

透過全方位的硬體與軟體保護產品組合，減少攻擊面並領先於現代威脅。

深入瞭解產品組合→

全球最安全的商用 AI PC[1] →

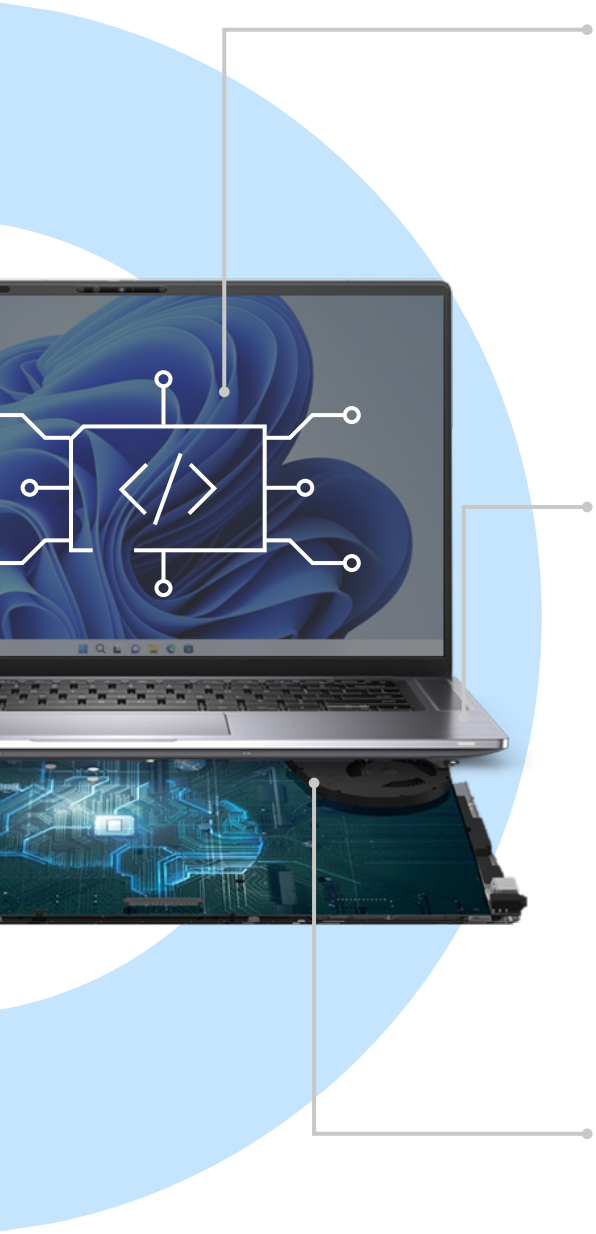
可改善任何機隊安全性的軟體 →

版權所有 © Dell Inc. 保留所有權利。

DELL Technologies

Dell Trusted Workspace

多層防禦



層疊式
軟體安全性

使用精選合作夥伴生態系統所提供的軟體，進一步強化進階威脅保護。充分運用整合式安全產品採購所帶來的優點和效率。

內建式
硬體與韌體安全功能

使用全球最安全的商用 AI PC，預防並偵測基本攻擊[1]。建立 BIOS/韌體和硬體層級的深度防禦，確保裝置在使用過程中始終受到保護。

Dell 獨家整合個人電腦遙測與業界領先軟體，全方位提升機群安全性。[1]

搭配式
供應鏈安全性

首次開機即確保裝置安全無虞，讓您放心工作。安全的個人電腦設計、開發及測試，有助於降低產品漏洞風險。嚴格的供應鏈控制可降低產品竄改風險。

預防、偵測及回應在任何地方出現的威脅

Dell SafeGuard and Response

Dell SafeData

持續提供保護來抵禦不斷變化的威脅

Dell SafeBIOS

Dell SafeID

信任硬體在交付時保持完好未被竄改

Dell SafeSupply Chain

版權所有 © Dell Inc. 保留所有權利。

DELL Technologies

Dell Trusted Workspace 搭配式及內建式安全性

全球最安全的商用 AI PC[1]

從第一次開機就安全無虞

嚴格且最先進的供應鏈控制和選用附加元件，例如 Dell 獨家 **Secured Component Verification**，可確保電腦完整性。

深入瞭解 →

保持 BIOS 的完整性

透過 Dell 獨家 BIOS Verification **SafeBIOS** 捕捉並擊退威脅。評估損毀的 BIOS、修復，並深入了解，進而減少未來面臨的威脅。

深入瞭解 →

驗證韌體完整性

Intel 處理器的硬體型安全性採用 Dell 獨家**韌體驗證**，可防止未經授權存取和高特權韌體竄改。

深入瞭解 →

找出潛在威脅

Indicators of Attack 是 Dell 獨家提供的早期警示功能，會掃描行為式威脅，以避免造成損害。

深入瞭解 →

安全的終端使用者認證

使用 Dell 獨家的專屬安全晶片 **SafeID** 驗證使用者存取，防止惡意軟體竊取使用者認證。

深入瞭解 →

捕捉已知漏洞

Dell 獨家 **Common Vulnerabilities and Exposures (CVE) Detection** 會監控是否有公開回報的 BIOS 安全性漏洞，並建議緩解風險的更新。

深入瞭解 →

Principled Technologies

*經 Principled Technologies 驗證的業界領先地位**

透過電腦遙測縮小 IT 安全性差距

以作業系統底層深入解析讓軟體解決方案更豐富。Dell 獨家整合電腦遙測與業界領先軟體供應商，全方位提升機隊安全性[1] 深入瞭解→

探索 Dell 受信任裝置

筆記型電腦 →

桌上型電腦 →

工作站 →

*研究結果僅適用於 Intel 架構裝置。

版權所有 © Dell Inc. 保留所有權利。

DELL Technologies

Dell Trusted Workspace 內建安全性

可改善任何機隊安全性的軟體

利用 Dell SafeGuard and Response 防堵進階網路攻擊

預防、偵測並回應在任何地方出現的威脅。人工智慧和機器學習會主動偵測並封鎖端點攻擊，安全性專家則可協助在端點、網路和雲端之間找出並補救已識別的威脅。

合作夥伴

CrowdStrike Falcon® →

Sophos | Secureworks® Taegis™ XDR →

利用 Dell SafeData 保護裝置與雲端上的資料

使用者隨時隨地都能夠安全協作。Netskope 針對雲端安全性和存取採用以資料為中心的方法，藉此保護各地的資料和使用者；Absolute 則是在企業防火牆之外提供 IT 可見度、保護和持久性。

合作夥伴

透過 Absolute 自我修復端點、應用程式和網路 →

透過 Netskope 探索安全服務邊緣解決方案 →

探索 Dell 安全性服務

Dell 客戶可自行管理安全性，或由專業人員為其管理。使用我們專為預防、回應並從 IT 環境中的安全性威脅恢復所設計的 360° SecOps 全方位管理解決方案。

深入瞭解 Managed Detection and Response Pro Plus →

版權所有 © Dell Inc. 保留所有權利。

DELL Technologies

Dell Trusted Workspace 硬體輔助安全性

整合式安全性

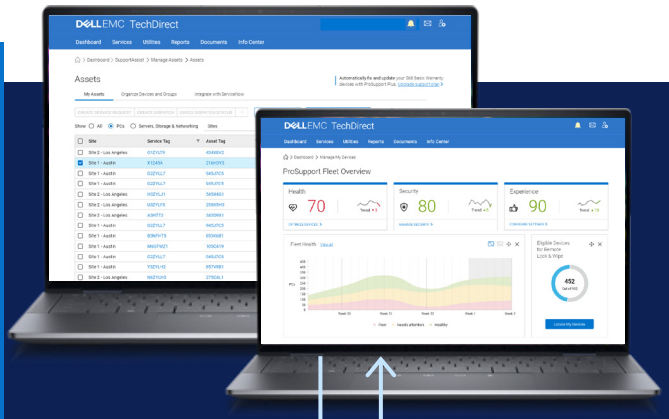
不斷演變的網路威脅會規避僅限軟體的防禦。透過硬體輔助保護協助縮小端點攻擊面。

為了防範現代威脅，硬體和軟體防禦必須共同合作。Dell 能提供這方面的協助。我們與業界領先的安全性合作夥伴共同合作，結合功能豐富、裝置層級的遙測功能和先進的威脅偵測能力，可改善您的機隊安全性。

- ✓ **縮小攻擊面**
- ✓ **改善威脅偵測能力**
- ✓ **維持裝置信任**
- ✓ **整合提供商**

層疊式
軟體安全性

只有 **Dell** 整合了電腦遙測功能與業界領先的軟體，以改善整個機隊的安全性[1 2]



作業系統

內建式硬體與韌體安全功能

Dell SafeBIOS

Dell Trusted Device 應用程式

BIOS Verification | CVE 偵測 | 攻擊指標

合作夥伴「作業系統之下」矽功能

搭配式
供應鏈安全性

Dell SafeSupply Chain[3]

裝置上 • 雲端上
安全元件驗證

版權所有 © Dell Inc. 保留所有權利。

DELL Technologies

使用 **Dell Trusted Workspace** 確保在任何地點都能安全工作。

搭配式及內建式安全性

層疊式軟體安全性

透過多層防禦功能，減少攻擊面並提升長期網路韌性。

期待與您相見
dell.com/endpoint-security

聯絡我們
global.security.sales@dell.com

瞭解詳情
端點安全性部落格 →

加入對話
LinkedIn/delltechnologies
X @delltech

資料來源與免責聲明

[1]根據 2024 年 10 月 (Intel) 和 2025 年 3 月 (AMD) 的 Dell 內部分析。適用於搭載 Intel 和 AMD 處理器的電腦。並非所有電腦均可使用所有功能。部分功能為選購。Intel 架構電腦經 Principled Technologies 驗證。《A comparison of security features》(安全性功能比較)，2024 年 4 月。[2]整合適用於 CrowdStrike Falcon Insight XDR 和 Absolute。[3]可用性因地區而異。

版權所有 © Dell Inc. 保留所有權利。

DELL Technologies