服務說明

Managed Detection and Response with Microsoft

簡介

Dell Technologies Services 很榮幸能根據本服務說明 (以下簡稱「服務說明」) 提供 Managed Detection and Response with Microsoft Service (以下簡稱「服務」)。您的報價單、訂單或雙方另行協定之形式的帳單或訂購確認函 (在適用情況下，以下簡稱「訂單」) 將載明您所購買服務的名稱和可用的服務選項。如需額外協助或索取服務合約副本，請聯絡技術支援或您的銷售代表。

本服務適用範圍

本服務的目的在於為客戶提供 Managed Detection and Response with Microsoft Service。

本服務以遠端方式提供。客戶應負責所有 Microsoft 授權和訂用方案；**Microsoft 授權不包含在本服務中。**請參閱**技術資料表**，以瞭解本服務的客戶資料量限制詳細資訊。

本服務的關鍵元件如表 1 所示：

表 1

購買的服務	本服務的關鍵元件
Managed Detection and Response with Microsoft	• 本服務利用 Microsoft Defender XDR 和 Microsoft Sentinel 技術來管理平台。 • 營運時間：一天 24 小時，一週 7 天 (24x7) • 服務啟動/啟用 • 租戶啟用與整備度 • 上線 • 偵測

購買的服務	本服務的關鍵元件
	• 威脅回應 • 與服務相關的安全性組態 • 季度報告 • 事件回應 • 包括上述元件，均充分利用客戶目前授權的 XDR 帳戶。 • 購買純服務方案的客戶必須滿足最低軟體模組要求才能享有服務。

注意：產品功能取決於客戶為保護客戶工作負載而購買的 Microsoft 授權/訂用方案；這將影響 Dell Technologies Services 團隊可用的補救選項。

營運時間

Dell Technologies Services 虛擬安全營運中心 (SOC) 的設計旨在為客戶提供一天 24 小時、一週 7 天 (24x7) 的服務。

本服務為客戶的 IT 環境提供完整解決方案，利用 Microsoft Defender 和 Sentinel 技術來管理平台，為裝置、網路、使用者活動、雲端應用程式和雲端資源提供安全防護。

服務的基線服務內容包括透過 Microsoft Sentinel 監控以下 Microsoft 元件：

監控範圍內的 M365 Defender 產品：

Microsoft Defender for Office 365

Microsoft Defender for Endpoint (最低必要服務)

Microsoft Defender for Servers (已上線至 Microsoft Defender for Endpoint)

Microsoft Defender for Identity

Microsoft Defender for Cloud Apps

案例管理/監控所需的先決條件

Microsoft Sentinel (最低必要服務)

注意：本服務需要專用的 Azure 訂用方案和工作空間。

租戶啟用與整備度服務會在一般上班時間提供。在客戶上線至 Dell 的全天候管理 SOC 之前，必須先完成租戶啟用與整備度程序。

表 2 列出了本服務關鍵元件的各要素。

表 2

關鍵元件	要素
服務啟動/啟用	• 服務啟用會議 (啟動會議) • 在 ITSM 平台建立客戶帳戶 • 服務參與前檢查清單 (由客戶完成)
租戶啟用與整備度	• 授權和訂用方案先決條件審查 • 部署前規劃 • Defender 原則審查/設定 • 連接器與資料來源 • 資料消化與日誌收集 • MDR 監控與報告
SOC 上線	• 審查客戶 IT 環境 • 服務啟用
偵測	• 全天候 24x7 安全性分析師服務 • 威脅偵測與調查 • Dell 啟動的威脅搜捕
威脅回應和安全性組態	• 威脅回應 • 與服務相關的安全性組態 • 與事件相關的遠端補救
季度報告	• 季度報告 • 安全性建議
事件回應	• 遠端事件回應啟動
專案管理	• 管理當次參與業務的交付事宜

詳細說明

服務啟動/啟用：

服務啟動會議

Dell Technologies Services 專案經理將召開會議，檢閱客戶對於服務的期待和需求，進而規劃服務交付事宜。服務啟動會議的目標為：

- 審查並討論客戶設定檔回應，以瞭解客戶的 IT 環境、安全性控管措施和其他相關背景關係。
- 針對客戶環境中目前的偵測機制，及客戶的應用方式提供指引。
- 提供與第三方軟硬體進行服務整合架構的指引。

萬一客戶另有超出本服務說明適用範圍的額外要求，協助處理這些要求的相關工作將視為額外服務，應收取額外費用。

服務參與前檢查清單 (由客戶完成)

審查 IT 環境前，客戶有責任完成服務參與前檢查清單中所列事項。Dell Technologies Services 專案經理會傳送服務參與前檢查清單給客戶，其中會詳載檢查清單與 IT 環境規格。

審查 IT 環境

執行 IT 環境審查此活動的目的在於，針對即將導入服務的客戶現有 IT 環境，收集相關資料。

租戶啟用與整備度

Dell Technologies Services 將針對支援本服務的核心元件提供指引。租戶啟用與整備度旨在確保客戶的 IT 環境符合提供全天候監控所需的最低組態。

Dell Technologies Services 將會根據對客戶 IT 環境的初步審查結果，為客戶提供 Defender 基線原則設定及 (如有需要) Sentinel 工作空間組態的指引。

請參閱**技術資料表**，瞭解有關本服務租戶啟用與整備度限制的其他詳細資訊。

租戶啟用與整備度概觀

1) 授權和訂用方案：確保客戶擁有 Microsoft 365 Defender 的必要授權和訂用方案。根據客戶的組織需求，確認是否需要額外的客戶授權。

2) 部署前規劃：檢閱客戶的安全性需求和現有基礎結構。

3) Defender 原則審查/設定：視需要在客戶的 Microsoft 365 管理入口網站中，啟動 Microsoft 365 Defender 元件。在客戶核准之下，協助設定 Defender 入口網站中的基線安全性設定。

4) 資料連接器、資料消化和記錄收集：將 Microsoft 365 Defender 與客戶的 Sentinel 環境整合，在可用且僅依客戶指示的情況下，集中管理安全性事件記錄和警示。針對支援的資料連接器提供導入方面的建議，以從 Microsoft Defender for Endpoint、Microsoft Defender for Office 365 和 Microsoft Defender for Identity 收集安全性資料。

5) MDR 監控與報告：使用 Microsoft Defender Security Center 將客戶 IT 環境的安全性狀態轉換為持續監控。

SOC 上線

服務啟用：

- 確認服務的租用先決條件
- 引導客戶完成隨需分配存取權限給 Dell Technologies Services 團隊的程序
- 引導客戶完成存取 M365 Defender XDR 所需的角色型存取控制 (RBAC) 指派程序

  注意：上述活動僅在 Microsoft Sentinel/Microsoft Defender for Servers (Microsoft Defender for Cloud) 在範圍內的情況下才適用。
- 引導客戶完成 Microsoft Sentinel 和 Azure Lighthouse 設定程序
- 引導客戶完成 Microsoft Sentinel 和 Azure Lighthouse 中用於管理 Defender for Servers 的 Microsoft Sentinel/Defender for Cloud ARM 範本設定程序
- 為客戶對安全事件的回應設置基本自動化規則/Playbook，以及任何所需的 SOC 自動化
- 調查和案件管理透過客戶的 Microsoft Sentinel/Defender 例項與 Dell 的 ServiceNow/ITSM 例項進行記錄。Dell Technologies Services 將與客戶合作配置此功能。任何與事件或服務相關的客戶請求或查詢，應透過 ServiceNow/ITSM 平台提出。

偵測

轉換為穩定狀態：

Dell Technologies Services 建議盡可能以最適宜的方式將客戶的 Defender 和 Sentinel 租戶上線，理想狀況是在服務開始後的一個月內完成 (不建議超過此時間)，以使本服務提供的深入見解和監控能力能發揮最大效用。

即時與歷史資料 (視 Microsoft 產品功能和儲存設定而定)：

- 經 Dell Technologies Services 判定為「真陽性」且需要客戶採取行動的相關安全性事件，將依下方詳述的服務等級呈報給客戶
- 判定為「偽陽性」或自動補救的事件將註記於客戶的季度報告中
- 在收到或建立 Dell Technologies Services 提供的自訂入侵指標時，將會進行分析

全天候 24x7 安全性分析師服務

Dell Technologies Services 安全性分析師 24x7 全年無休，可針對相關問題提供協助。

威脅偵測與調查

審查並調查 XDR 應用程式內偵測到的威脅。如 Dell Technologies 判定需進一步分析威脅，便會在 Microsoft Defender XDR 和 Sentinel 應用程式內建立調查。如 Dell Technologies 已收集充足證據可將威脅視為惡意，或需要客戶提供更多資訊才能繼續調查，將會透過 XDR 入口網站、電子郵件或支援的整合架構來聯絡客戶。

威脅搜捕

Dell Technologies 會在客戶的 IT 環境中執行威脅搜捕，以便從目前的事件回應參與中收集到的漏洞和戰術搜尋相關指標。威脅搜捕活動僅限於透過 XDR 平台收集到的資料。Dell Technologies 會檢查所收集的客戶遙測資料，以偵測持續性機制的存在與否、異常使用者活動、威脅行為者戰術、異常網路通訊，以及異常應用程式使用量等活動。在威脅搜捕程序中偵測到的威脅將促使我們透過 XDR 入口網站、電子郵件或支援的整合架構建立調查，並通知客戶。

威脅回應

在上線期間，客戶將預先核准可作為服務一部分而採取的特定威脅回應動作。Dell Technologies Services 將利用 XDR 平台執行威脅回應動作。

與服務相關的安全性組態

在服務期限內，Dell Technologies Services 每季可視需要核准最多 40 小時的服務相關遠端安全性組態來協助客戶。安全性組態專限定於因提供服務所產生的調查和/或警示，且可能包括：

- MDR 端點代理程式故障診斷和最佳實務指引。
- 針對 XDR 平台原則的更新提供指導。
- 引導設定第三方應用程式，並整合至 XDR 平台。

在服務期限內，每季至少應提供 40 小時的服務相關威脅回應和安全性組態協助，客戶可與他們的 Dell Technologies 業務經理商討並購買額外時數。在服務期限的季度結束時，我們將收回未使用的任何時數。在服務期限的未來季度開始前，無法使用為該季度額外購買的時數。

季度報告

Dell Technologies Services 每季將透過服務平台，針對客戶 IT 環境中所觀察到的趨勢和顯著活動提供報告，並就如何抵禦威脅給予建議。季度報告包括調查和警示趨勢、分析及安全狀態指引的概述。

事件回應

一旦收到 Dell Technologies Services 安全性分析師的通知，即可使用下列遠端事件回應元件。

遠端事件回應啟動

在服務期限內，Dell Technologies Services 每**年**將提供客戶最多 40 小時的遠端事件回應協助，且限定所監控的端點數量範圍。包括但不限於以下協助：

- 建立事件回應服務的單一聯絡窗口
- 啟動分析客戶的內部部署和雲端基礎結構，其中可能包含：
    - 主機資料
    - 網路資料
    - 惡意程式碼
    - 記錄資料，以及
    - 網路威脅情報
- 數位媒體處理指引和支援的初步分析與協調
- 初步狀態報告和行動項目追蹤
- 必要補救和後續步驟的初步概觀

在服務期限內，每年至少應提供 40 小時的遠端事件回應協助，客戶可與他們的 Dell Technologies 業務經理商討並購買額外時數。在服務期限的年度結束時，我們將收回未使用的任何時數。在服務期限的未來年度開始前，無法使用為該年度購買的時數。

專案管理

Dell Technologies Services 將指派專案經理 (PM) 作為單一聯絡窗口 (以下稱「SPOC」)，以管理當次業務參與的交付事宜。

- 成功交付服務的單一連絡人負責制。
- 對時間、成本及服務範圍的持續專注。

- 協調並促成啟動、狀態、交付項目審查和結案會議。
- 建立並管理服務時程表、溝通以及狀態回報。
- 視需要促進變更管理。
- 確認交付的服務符服務說明。
- 取得客戶的交付項目和服務完成驗收。
- 管理客戶關係。
- 專案管理活動以遠端進行。

訂用方案費用

本服務提供每月訂用方案費用，如果客戶已選擇收取帳單，即會載明於「原訂單」，並加註「訂用方案」字樣。否則，可套用標準條款和發票開立程序。以下條款適用於訂用方案費用：

- 原訂單將載明合約期限和簽訂的端點數量。服務期限過後將自動續訂相同條款。
- 客戶提交其他端點的訂單，即可增加受管理端點的數量。這些額外端點將與客戶現有的受管理端點合併，形成新的「端點總數」。
- 我們將事後按月開立端點總數的發票給客戶，並在行事曆的月底受管理這些端點。
- 在任何情況下，客戶都不能將受管理端點的數量減低到總端點數以下，總端點數也不能為了發票開立而減量
- 客戶將取得使用本服務的客戶端點報告。
- 客戶會收到 (相同地區內) 所有位置的單一發票。
- 客戶必須在客戶的自動續訂服務期限終止前的六十 (60) 天，提供書面聲明給 Dell Technologies。

資料量和使用限制

本服務使用客戶的 Microsoft Sentinel、Azure 和 Microsoft Defender XDR 租戶，以及客戶託管的專用 Azure 訂用方案和服務工作空間。購買本服務的客戶有責任瞭解及管理本身的資料量和使用限制，Dell Technologies Services 對客戶不具任何此類相關責任或義務。客戶也應瞭解，與其 Azure 訂用方案和 Sentinel 工作空間相關的所有資料儲存和運算成本需由其負責。

資料儲存位置

購買本方案的客戶有責任自行確認其資料儲存位置。M365 區域和設定的工作空間資料位置會依客戶指示並由其決定，設在客戶的 Microsoft Azure 環境中。

Microsoft Sentinel 會將客戶資料儲存在其工作空間組態中定義的區域中。Microsoft 會將客戶資料和與客戶 Microsoft Sentinel 環境相關聯的記錄分析工作空間，儲存在相同的地理位置。

Microsoft Sentinel 處理客戶資料的位置為以下兩地之一：

- 如果記錄分析工作空間位於歐洲，則在歐洲處理客戶資料。
- 所有其他位置的客戶資料會在美國處理。

服務等級

Dell 會根據多項服務等級來衡量其威脅回應和解決方案效能。

計量	定義	目標
平均反應時間	從高度或嚴重警示產生的時間到 XDR 應用程式中建立調查的時間所測得的平均時間。	15 分鐘
平均回應時間	從調查建立的時間到 Dell 分析師在 XDR 應用程式中提供初始事件分析或向客戶提供回應時所測得的平均時間。	60 分鐘
平均解決時間	從 XDR 應用程式中建立調查的時間到調查解決的時間所測得的平均時間。	24-48 小時 (需要客戶協同合作)

假設

記錄本服務說明中詳述的各項服務時，Dell Technologies Services 秉持下列假設：

1. 客戶提供的所有現場技術需求及架構資訊皆正確無誤。
2. Dell Technologies Services 僅會實施 Dell 變更管理程序所允許的服務相關安全性組態變更。
3. 客戶未遵循變更管理程序即實施的任何原則變更，Dell Technologies Services 概不負責。
4. 服務說明所述的所有服務會以遠端方式執行。
5. Dell Technologies Services 會透過 Microsoft Sentinel 儀表板來管理環境。
6. 產品功能取決於客戶為保護客戶工作負載而購買的 Microsoft 授權和訂用方案；這將影響 Dell Technologies Services 團隊可用的補救選項。舉例來說，若要保護伺服器，Defender for Server Plan 1 為建議的最低基線。然而，Defender for Server Plan 2 可為伺服器提供更多的保護，並增加更多的 Microsoft Defender for Cloud 功能。
7. Dell 保留在新功能推出時，變更案例管理/ITSM 解決方案的權利。

8. 客戶端點計數將根據 Sentinel 中監控的端點數量來計算。
9. 至少 40% 的端點感應器部署到授權的端點後，Dell Technologies Services 便會將客戶從 SOC 上線移至穩定狀態監控。
10. 萬一服務無法於指定的期間內如期完成，Dell Technologies Services 保留評估根本原因的權利。若此根本原因非屬 Dell Technologies Services 的掌控範圍內，Dell Technologies Services 會提出解決此延遲情形的因應措施。這些措施可能需要客戶購買額外服務或支付額外費用，以便 Dell Technologies Services 完成本服務。萬一客戶另有超出本服務說明適用範圍的額外要求，協助處理這些要求的相關工作將視為額外服務，應收取額外費用。
11. Microsoft Sentinel 生態系統具有高訊噪比，因此偽陽性比率較低；Dell Technologies Services 在調查高和中嚴重性警示之後，會根據大量的同類型警示，調查資訊警示和低嚴重性警示。

排除項目

雖然本服務旨在協助客戶識別和降低風險，但無法完全排除風險。因此，Dell Technologies Services 無法保證客戶 IT 環境中不會發生入侵、外洩或其他未經授權的活動。

為避免疑義，以下活動不包含在本服務說明的適用範圍內：

1. 本「服務說明」中未特別註明的任何服務、任務或活動。
2. 服務不包括專門為客戶開發任何智慧財產權。
3. 故障診斷或修正任何現有系統/伺服器問題 (除非本「服務說明」另有說明)，包括但不限於 M365 Defender 感應器或 Microsoft Sentinel 支援的代理程式瑕疵。
4. 測試 Dell Technologies 產品與其他第三方產品的整合性，例如但不限於協力廠商的加密或安全性產品。
5. 除非本「服務說明」另有說明，否則服務不包括補救或改善任何於分析客戶環境時發現的效能問題。
6. 除非本「服務說明」另有說明，否則無論任何情況下，Dell Technologies Services 的責任 (包括財務方面的責任) 並不涵蓋任何客戶和/或第三方人員、硬體、軟體、設備或客戶作業環境目前使用的其他資產。
7. 解決製造商無法解決的相容性問題或其他問題，或設定與製造商支援之設定相衝突的軟硬體、設備或資產。
8. 資訊警示和低嚴重性警示的監控不在本服務範圍內。
9. 安裝或設定系統記錄伺服器或系統記錄/CEF 收集器。
10. 設定 Microsoft Defender for Cloud Apps 應用程式。
11. 監控未包含在 Microsoft Defender for Servers Plan 1 或 Plan 2 授權中的 Microsoft Defender for Cloud 功能。

12. 監控尚未作為服務的一部分上線的任何伺服器。Dell Technologies 不會對已上線伺服器以外的任何實體相關警示進行分級。
    a. 注意：這僅適用於範圍內的伺服器/ Defender for Cloud。

服務特定的客戶責任

客戶同意就其服務交付事宜與 Dell Technologies Services 合作，並同意以下責任：

1. 在 XDR 平台中提出變更要求時遵循變更管理程序，並向 Dell Technologies Services 提供將核准變更管理要求的客戶聯絡人。
2. 在服務期間，向 Dell Technologies Services 分析師提供進入所有必要客戶環境的權限。
3. 提供客戶指定代表，該代表將出席所有規劃與檢討會議。
4. 提供允許 Dell Technologies Services 代表客戶管理 XDR 平台所需的各種授權 (包括第三方授權)。
5. 使用適當的應用程式部署工具 (如 Intune、SCCM 等)，將代理程式/感應器部署到客戶所有的授權端點。
6. 參與適當的服務隨需分配。客戶瞭解如未適度參與 (包括目標設定)，技術人員將無法滿足客戶需求或執行服務。
7. 配合 Dell Technologies Services 分析師並遵循其指示。
8. 檢閱並同意服務參與前檢查清單和測試計畫。
9. 請確定客戶 IT 環境設有支援的端點代理程式，且已安裝在服務授權的主機上。
10. 從第三方或其他授權來源取得第三方端點代理程式的所有支援；Dell Technologies Services 不提供第三方端點代理程式的支援。
11. 移除或新增衝突第一方和/或第三方防毒軟體和 EDR 代理程式的例外情況，以便 Dell Technologies Services 能夠提供本服務。
12. 確保可取得充足的可用網路頻寬以執行服務。
13. 請確定所有的裝置整合皆能正常運作，並能持續適當運作。如果客戶需要，Dell Technologies Services 可收費協助。
14. 提供適當 XDR 應用程式存取權以進行整合。
15. 確保客戶安全性控管措施與 XDR 整合架構相容。
16. 管理登入資料和權限，以便透過 XDR 應用程式進行整合。
17. 確保客戶的授權連絡人清單處於最新狀態，包括權限及相關資訊。
18. 在 Dell Technologies Services 進行威脅調查期間，提供即時資訊和協助 (例如檔案、記錄、IT 環境背景)。
19. 識別並驗證所有服務的客戶授權使用者。

20. 控制使用者的未經授權存取，並維持使用者名稱、密碼和帳戶資訊的機密性。
21. 對客戶授權使用者所有的活動負責，如有任何未經授權的服務使用行為，也應立即通知 Dell。
22. 使用雙因素驗證 (若有) 存取本服務。
23. 接受端點代理程式的所有必要更新和升級，以利於本服務的正常運作和安全性。
24. 視需要向 Dell Technologies 提供服務服務中斷期間。
25. 控制資料存取，防止跨用戶端資料傳授，並抑制客戶環境中的資料遺失或資料外洩風險。
26. 維持本服務支援的受管理端點的正確數量。
27. 設定 Microsoft Sentinel Azure 訂用方案並隨需分配 Dell 分析師所需的存取權限。這是本服務的先決條件。
28. 透過 Microsoft Sentinel 提供 Microsoft 365 Defender 的存取權，將藉由客戶傳送給 Dell 分析師的 Microsoft Entra ID B2B 邀請隨需分配。
29. 客戶環境的實體及網路安全性。
30. 除非雙方另有約定，否則應根據 DT Services 標準範本提供所有文件。
31. 提供至少兩 (2) 個級別的呈報聯絡人，以便及時回應 Dell 呈報事宜。客戶應提供可在假日和非營業期間聯絡的呈報聯絡人。
32. 維護 Microsoft Sentinel 儀錶板的運行狀況、調整和組態。
33. 提交技術支援工單給 Microsoft 以解決問題。Dell Technologies Services 不會提供第三方端點代理程式的支援。
34. 決定要送至 Microsoft Sentinel 進行消化的客戶安全性資料量。
35. 監控針對非伺服器實體產生的警示。
36. 移除任何第一方/第三方 AV/EDR 代理程式。
37. 提供 DT Services 執行本服務所需的任何必要同意。
38. 所有資料保留和運算成本。
39. 設定原則設定以滿足客戶需求。
40. 新增整合架構和資料來源至受管理的 MDR 平台。
41. 必須提供專用的 Azure 訂用方案，才能透過 Microsoft Sentinel 提供案例/意外管理、調查和季度報告。
42. 將 Android 和 iOS 裝置上線。請注意，每部受監控的手機均視為本服務中監控的一個端點。

詞彙表

表 3

術語	說明
警示	MDR 應用程式觀察到可疑或惡意行為的優先順序。
案例管理	用於調查和管理安全性事件與警示的集中式平台。
變更管理	客戶環境中的受控識別、實作和必要變更核准。
端點代理程式/感應器	安裝在端點上的應用程式，用於收集端點的活動和作業系統詳情等相關資訊，繼而傳送至安全性應用程式進行分析並偵測威脅。
Endpoint Detection and Response (即「EDR」)	一款安全性平台，使用第一方端點代理監控最終使用者裝置 (桌上型電腦、筆記型電腦、平板電腦和手機) 是否存在防毒軟體無法偵測到的威脅。
Extended Detection and Response (即「XDR」)	超越傳統端點 (雲端、OT、網路等) 的偵測與回應平台。XDR 平台使用整合或連接器來消化原生、第三方或服務導向的資料，這些資料會交叉關聯形成安全性監控背景。
事件回應	為緩解已識別資安事件而採取的回應操作。
整合	應用程式發展介面 (API) 呼叫或其他軟體指令檔，用以進行連線技術的合意服務。
調查	中央位置，用以收集與威脅有關的證據、分析和建議，此威脅可能鎖定客戶 IT 環境中的某資產。
Managed Detection and Response (即「MDR」)	由 Dell MDR 方案支援的安全性應用程式。技術詳細資訊請參閱技術資料表。
安全性事件	發生涉及客戶的外洩或可疑攻擊的情況。
安全性原則	XDR 平台的原則，會在客戶環境中強制執行防範和偵測設定。
安全性組態	MDR 包含每季 40 小時的服務，為客戶提供調查或與警示相關的回應行動。

術語	說明
租戶啟用與整備度	提供啟用服務所需核心元件的指引。租戶啟用與整備度旨在確保客戶的 IT 環境符合提供全天候監控所需的最低組態。
威脅	MDR 應用程式識別的任何活動，可能會對客戶 IT 環境中的某資產造成損害。
威脅搜捕	軟體和人員在 IT 環境內尋找先前未成功識別的威脅之循環程序。
威脅回應	XDR 應用程式提供的平台內回應，例如隔離主機或封鎖檔案 (遏止類型行動)。

一般客戶責任

存取權限的授權單位。客戶聲明並保證，其已為本身及 Dell Technologies Services 取得權限，得以遠端或現場存取及使用客戶擁有或取得授權之軟體、硬體、系統與其資料，以及所有上述項目所包括的硬體和軟體元件，以達提供各項服務之目的。如果客戶尚未取得上述使用權限，在客戶要求 Dell Technologies Services 執行服務之前，客戶應負責取得所需權限並支付相關費用。

競業禁止。即使法律允許，但若未事先取得 Dell Technologies Services 的書面同意，自訂單上所載日期起 2 年內，客戶不得直接或間接挖角客戶在 Dell Technologies Services 執行服務相關事宜時接觸到的 Dell Technologies Services 員工；惟一般徵才廣告及其他類似的招募形式並不構成此處所述之直接或間接挖角，且已在與客戶進行僱用討論之前即解僱或離職的 Dell Technologies Services 員工，亦不在限制之內。

客戶合作。客戶瞭解，若未能迅速且充分地配合，Dell Technologies Services 將無法履行服務；或即使履行，服務也可能發生重大變動或延遲。因此，客戶將迅速並合理地為 Dell Technologies Services 提供履行服務所需的合作。如果客戶未能按照前述規定合理且充分地配合，若有任何未能履行服務之情況，Dell Technologies Services 概不負責，且客戶亦無權申請退款。

現場義務。若服務需要現場履行，客戶應無償提供工作場所和環境讓 Dell Technologies Services 安全地充分使用，包括充足的工作空間、電力、安全設備 (如適用) 與市內電話。若系統原本並未配備顯示器、滑鼠 (或指向裝置) 和鍵盤，則應另行提供 (不得向 Dell Technologies Services 收取任何費用)。

資料備份。在提供本服務之前及服務期間，客戶將完成受影響之系統中所有現有資料、軟體與程式之備份。客戶應定期備份所有受影響系統上所儲存之資料，為可能發生的故障、變更或資料遺失採取預防措施。Dell Technologies Services 不負責復原或重新安裝任何程式或資料。

除非適用之當地法律另有規定，否則 Dell Technologies Services 對下列項目概不負責：

- 您的任何機密、專屬或個人資訊；
- 資料、程式或軟體遺失或損毀；
- 損壞或遺失的可移除媒體；
- 無法使用的系統或網路；及/或
- Dell Technologies Services 或第三方服務提供者之任何行為或疏失 (包含過失)。

第三方保固。Dell Technologies Services 提供此等服務時，可能需要存取非 Dell Technologies Services 製造或販售的硬體或軟體。部分製造商的產品，可能會因 Dell Technologies Services 或其他非原廠人員對軟硬體執行作業而導致產品保固失效。客戶應負責確保 Dell Technologies Services 所執行的服務不會影響此類保固，或保固受到影響，客戶也可以全然接受。第三方保固或因本服務而對保固造成的任何影響，Dell Technologies Services 概不負責。

排除資料。「排除資料」意指：(i) 機密資料，用於美國軍事管制清單 (包括軟體與技術資料)；或兩者；(ii) 列為國防軍品和國防服務之物品、服務及相關技術資料；(iii) ITAR (國際武器交易條例) 公佈的資料；以及 (iv) 因客戶內部政策、慣例、產業專用標準或法律，而受到更高安全性規範之個人可識別資訊。客戶瞭解本服務目的必非處理、儲存排除資料，或用於相關情形。客戶應全權負責審閱將提供給 Dell Technologies Services 或由 Dell Technologies Services 存取的資料，確保其中不含排除資料。

服務時間。除了以下另行列出者，租戶啟用與整備度服務遵循當地每週工作時數相關法律之規定，於週一至週五在 Dell Technologies Services 一般上班時間內執行，亦即客戶當地時間上午 8 點至下午 6 點：

國家/地區	**一般 Dell Technologies Services 上班時間**
聖克里斯多福、聖露西亞、聖文森、千里達、維京群島、通行英語的其他加勒比海國家/地區	週一至週五，上午 7 點至下午 4 點
巴貝多、巴哈馬、貝里斯、哥斯大黎加、丹麥、薩爾瓦多、芬蘭、開曼群島、瓜地馬拉、宏都拉斯、牙買加、挪威、巴拿馬、波多黎各自治邦、多明尼加共和國、蘇利南、瑞典、土克斯及開科斯群島	週一至週五，上午 8 點至下午 5 點
澳洲、百慕達、中國、海地、日本、荷屬安地列斯群島、紐西蘭、新加坡、泰國	週一至週五，上午 9 點至下午 5 點
阿根廷、巴西、厄瓜多、法國、印度、印尼、義大利、韓國、馬來西亞、墨西哥、巴拉圭、秘魯、台灣、烏拉圭	週一至週五，上午 9 點至下午 6 點
玻利維亞、智利	週一至週五，上午 9 點至下午 7 點
中東地區	週日至週四，上午 8 點至下午 6 點
香港特別行政區	週一至週五，上午 9 點至下午 5 點 30 分

除非事先已有書面約定，否則非當地一般上班時間或國定假日期間均不提租戶啟用與整備度服務。

服務條款與條件

本服務說明是由客戶您 (下稱「您」或「客戶」) 與本服務訂購表單上所載公司 (下稱「Dell 公司」) 共同簽訂。本服務受客戶與 Dell 公司另行簽訂之主服務協定所規範，該協定內文明確授權本服務銷售事宜。若無此等協議，則根據客戶所在地點而定，本服務受 Dell「商業銷售條款」或下表中提及之協議 (若適用，簡稱「協議」) 所約束規範。您的客戶位置適用的 URL 清單請參閱下表，您可以從中找到您的協議。雙方在此確認已詳閱並同意遵守這些線上條款。

客戶位置	您購買服務所適用的條款與條件	
	客戶直接購買服務	客戶透過授權經銷商購買服務
美國	Dell.com/CTS	Dell.com/CTS
加拿大	Dell.ca/terms (英文) Dell.ca/conditions (法文-加拿大)	Dell.ca/terms (英文) Dell.ca/conditions (法文-加拿大)
拉丁美洲與加勒比海地區	當地的線上商業銷售條款，位於國家/地區專有的 Dell.com 網站或 Dell.com/servicedescriptions/global。*	服務說明和您可能從銷售方取得之其他 Dell 公司服務文件，並不構成您與 Dell 公司之間的協定，僅能用於說明您自銷售方購買之服務內容、得到服務所應善盡之義務，以及此類服務之限制。因此，本服務說明及其他任何 Dell 公司服務文件中所提及之任何「客戶」，在此上下文中，應理解為您本人，而任何提及的 Dell 公司，應僅理解為代表您服務提供者提供服務之 Dell 公司。此處所述之服務，您與 Dell 公司並無直接合約關係。為避免疑義，本質上與購買方和銷售方直接相關之任何支付條款或其他合約條款並不適用於您，而應由您與銷售方達成相關協議。
亞太地區-日本	國家/地區專有的當地 Dell.com 網站或 Dell.com/servicedescriptions/global.*	服務說明和您可能從銷售方取得之其他 Dell 公司服務文件，並不構成您與 Dell 公司之間的協定，僅能用於說明您自銷售方購買之服務內容、得到服務所應善盡之義務，以及此類服務之限制。因此，本服務說明及其他任何 Dell 公司服務文件中所提及之任何「客戶」，在此上下文中，應理解為您本人，而任何提及的 Dell 公司，應僅理解為代表您服務提供者提供服務之 Dell 公司。此處所述之服務，您與 Dell 公司並無直接合約關係。為避免疑義，本質上與購買方和銷售方直接相關之任何支付條款或其他合約條款並不適用於您，而應由您與銷售方達成相關協議。

客戶位置	您購買服務所適用的條款與條件	
	客戶直接購買服務	客戶透過授權經銷商購買服務
亞太地區-香港特別行政區	https://www.dell.com/learn/hk/zh/hkcorp1/legal_terms-conditions_dellgrmwebpage/commercial-terms-of-sale-hk-en-zh?c=hk&l=zh&s=corp&cs=hkcorp1	服務說明和您可能從銷售方取得之其他 Dell 公司服務文件，並不構成您與 Dell 公司之間的協定，僅能用於說明您自銷售方購買之服務內容、得到服務所應善盡之義務，以及此類服務之限制。因此，本服務說明及其他任何 Dell 公司服務文件中所提及之任何「客戶」，在此上下文中，應理解為您本人，而任何提及的 Dell 公司，應僅理解為代表您服務提供者提供服務之 Dell 公司。此處所述之服務，您與 Dell 公司並無直接合約關係。為避免疑義，本質上與購買方和銷售方直接相關之任何支付條款或其他合約條款並不適用於您，而應由您與銷售方達成相關協議。
歐洲、中東及非洲	國家/地區專有的當地 Dell.com 網站或 Dell.com/servicedescriptions/global。* 此外，位於法國、德國和英國的客戶，可以選擇下列適用的 URL： 法國：Dell.fr/ConditionsGeneralesdeVente 德國：Dell.de/Geschaeftsbedingungen 英國：Dell.co.uk/terms	服務說明和您可能從銷售方取得之其他 Dell 公司服務文件，並不構成您與 Dell 公司之間的協定，僅能用於說明您自銷售方購買之服務內容、得到服務所應善盡之義務，以及此類服務之限制。因此，本服務說明及其他任何 Dell 公司服務文件中所提及之任何「客戶」，在此上下文中，應理解為您本人，而任何提及的 Dell 公司，應僅理解為代表您服務提供者提供服務之 Dell 公司。此處所述之服務，您與 Dell 公司並無直接合約關係。為避免疑義，本質上與購買方和銷售方直接相關之任何支付條款或其他合約條款並不適用於您，而應由您與銷售方達成相關協議。

*客戶如需存取所在地的 Dell.com 網站，只需從當地連上網際網路的電腦存取 Dell.com，或在 Dell 網站的「選擇國家/地區」(網址 Dell.com/content/public/choosecountry.aspx?c=us&l=en&s=gen) 中選擇合適的選項即可。

客戶亦進一步同意，合約效期屆滿後，凡續約、修改、延長或繼續使用服務，均以當時最新的服務說明為依據 (如需瞭解內容，可前往 Dell.com/servicedescriptions/global 查詢)。

若構成本合約的任何文件條款之間有所牴觸，條款效力將適用下列順序：(i) 本服務說明；(ii) 合約；(iii) 訂單。現行條款會儘可能限縮解釋，以利解決牴觸之處，並儘可能保留不相牴觸的條款，包括保留相同段落、章節或子章節中不相牴觸的條款。

一旦確立服務訂單、收到服務、使用服務或相關軟體，或在與購買產品相關之 Dell.com 或 DellEMC.com 網站，或 Dell Technologies 軟體或網際網路介面上點選/勾選 [I Agree] (我同意) 按鈕、方塊或類似選項時，即代表您同意遵守本服務說明，以及納入其中以供參考之合約。如果您代表公司或其他法人公司實體簽訂本服務說明，即表示您有權約束此類實體遵守本服務說明，此處之「您」或「客戶」係指此類實體。除收到本服務說明外，位於某些國家/地區的客戶可能還必須履行已簽署的訂單。

資料收集和使用聲明

本聲明 (簡稱「聲明」) 闡明了 Dell Technologies 及其事業群如何在您使用 Dell 軟體時，代表自身或為第三方或為其直接與間接子公司 (簡稱「Dell」) 收集、使用和共享您的資料。我們收集並使用某些類型的資料 (如下所述)，以便在您使用 Dell 產品時提供個人化的使用體驗，繼而增強我們的支援並改善我們的產品、解決方案和服務 (統稱「Dell 解決方案」)。

我們已收集的資訊。我們可能會就您使用、存取 Dell 解決方案或與之互動的方式，自動收集行為與使用資訊。此資訊不一定能直接顯示您的身份，但可能包含唯一的身份識別符和其他您使用之特定裝置的相關資訊，例如您的產品服務編號、硬體型號、作業系統版本、硬體設定和系統當機記錄、已安裝的應用程式、其設定和使用量，及/或 (MAC) 位址，以及可識別專屬於您的裝置或系統的其他資料。

我們可能也會收集您的系統或裝置如何與 Dell 解決方案互動的相關資訊，例如統計資訊、網路連線指標和路由，或在使用 Dell 服務的情況下，與安全性事件有關的資訊。在某些情況下，收集到的資訊可直接或間接識別最終使用者，並在本聲明提供的目所需限度內，建立個別使用者與特定線上行為的關聯。

為了支援這些活動，您同意授予 Dell 有限、非專屬授權，以使用您的資料執行此服務。您亦同意授予 Dell 有限、非專屬、永久、全球、不可撤銷的授權，以在服務期間和服務期間後使用和以其他方式處理與安全性事件相關的資料，以開發、強化及/或改善我們提供給客戶的服務和 Dell 解決方案。Dell 無須基於任何理由在此服務終止時退回或刪除與安全性事件相關的資料。

[Dell 軟體可在建立網際網路連線時，將上述全部或部分資訊整合進資料紀錄中並傳給 Dell。]

Dell 所用的技術類型可能會隨著技術的演進與時俱進。如需更多使用 Cookie 和其他類似追蹤技術的資訊，請至 Dell 的線上隱私權聲明參閱我們的 Cookies 和類似技術。

資料傳輸。本聲明中所述資料可能會傳輸到所在國家/地區以外的其他位置，例如美國、歐盟、日本，包括第三方主機受管理的場所。我們將採取所有適當的技術與組織措施來保護我們傳輸的資料。

資料保留。鑒於本聲明中所述目的，並依據 Dell 的保留原則和適用法律之必要，我們將保留您的個人資料。根據 Dell 的保留原則和適用法律，本聲明中所述由 Dell 收集的資料將予以保留。

個人資訊和隱私權。Dell 收集、使用和處理您提供的個人資訊之行為如 Dell 的隱私權聲明中所述。若因任何理由而要聯絡我們，瞭解我們的隱私權慣例，請寄送電子郵件至 privacy@dell.com，或至 https://www.dell.com/learn/us/en/uscorp1/policies-privacy-country-specific-privacy-policy 參見我們的完整線上隱私權聲明。

補充條款與條件

1. 服務條款。本服務說明自訂單上所載日期起開始生效，直至訂單指定的期限 (以下稱「**期間**」) 結束為止。倘若適用，只要客戶購買一或多項服務，客戶的訂單上皆應載明其購買之系統、授權、安裝、部署、管理端點或最終使用者數量、費率或價格，以及各服務的適用期限。除非 Dell Technologies Services 與客戶另行簽署書面合約達成共識，否則客戶購買本服務說明所述的服務，僅供客戶內部使用，不得轉售或用以對外提供服務。

2. 其他重要資訊

A. 重新排程。一旦本服務日期排定後，任何排程變更都必須在排定日期的至少 8 天前提出。如果客戶在原定日期 7 天之內重新排定日期，則須支付重新排程費用，該費用以不超過服務價格 25% 為上限。客戶須在服務開始前至少 8 天確認任何重新排程的服務。

B. 購買硬體與服務之付款規定。除非另行簽署書面合約達成共識，否則在任何情況下，硬體貨款不得以其一併購買的服務之效能或交付情形為付款條件。

C. 商業上合理之服務範圍限制。若 Dell Technologies Services 依據商業常理判斷，認定提供服務會對 Dell Technologies Services 或 Dell Technologies Services 的服務提供者造成不合理風險，或有任何要求的服務超出服務範圍，Dell Technologies Services 得拒絕提供服務。若因 Dell Technologies Services 無法掌控的原因，包括客戶未能遵守本服務說明所述的自身義務，而導致 Dell Technologies Services 無法提供服務或延遲服務，則 Dell Technologies Services 概不負責。

D. 選用服務。客戶可向 Dell Technologies Services 購買選用服務 (包括需求點支援、安裝、諮詢、管理、專業、支援或訓練服務)，而 Dell Technologies Services 提供的選用服務會依客戶所在地點而異。購買選用服務可能需與 Dell Technologies Services 另外簽署合約。如未另訂協議，則選購服務將依本服務說明規定。

E. 轉讓與外包。Dell Technologies Services 得將本服務外包和/或分派給合格的第三方服務提供者，由其以 Dell Technologies Services 名義提供服務。

F. 取消服務。服務期間內，Dell Technologies Services 得因下列任一原因隨時取消本服務：

- 客戶無法在發票期間內支付本服務的全額費用；
- 客戶濫用、威脅或拒絕協助分析師或現場技術人員；或者
- 客戶未遵守本服務說明所載之任何條款和條件。

若 Dell Technologies Services 取消本服務，Dell Technologies Services 會將書面取消通知寄送至客戶發票所載地址。通知內容包括取消服務的理由，以及取消服務的生效日期，該生效日應為 Dell Technologies Services 寄送取消通知給客戶當日起十 (10) 天以上；若當地相關法律另有規範，則從其規定。若 Dell Technologies Services 依本條規定取消本服務，客戶無權對已支付給 Dell Technologies Services 之費用或應付款項要求退費。

G. 地區限制與地址遷移。並非所有地點都能提供本服務。服務選項 (包括服務等級、提供技術支援時段、服務特色和功能，以及現場回應時間) 依地理地區而異。此外，客戶所在地可能無法購買特定選項。如需詳細資訊，請洽詢您的銷售代表。