SOPHOS MDR（託管式威脅偵測與應變）服務簡介

在數位轉型與混合辦公模式成為常態的情況下，企業正面臨前所未有的資安挑戰。使用者、裝置與資料高度分散，使攻擊面持續擴大，而威脅手法也日益進階且自動化。對多數 IT 與資安團隊而言，僅仰賴傳統工具與人力，已難以有效因應現今快速演變的威脅環境。企業常常面臨以下問題：

- **資安人力短缺與高負擔**：專業資安人才難以招募與留任，高壓工作型態也容易導致疲勞與倦怠。
- **缺乏 24/7 監控能力**：許多組織在非上班時間無法即時偵測與回應威脅，錯失阻止攻擊的關鍵時機。
- **警示雜訊過多，難以判斷優先順序**：來自多套系統的大量警示，使 IT 團隊難以快速識別真正的高風險事件。
- **資料孤島與工具整合不足**：資安資訊分散於不同系統，無法形成完整威脅視角，影響事件分析與處置效率。
- **高度仰賴人工與被動回應**：手動關聯事件與事後回應模式，讓攻擊者有更多時間擴大影響。

在威脅持續升級且資源有限的現實下，企業需要的不只是更多工具，而是更有效率與可持續的資安營運模式。透過整合式、具備全天候監控與專家主導回應能力的解決方案，組織才能降低營運風險、提升防護成熟度，並從被動防禦轉向更主動、前瞻的資安策略。由於上述威脅與維運挑戰，組織正日益轉向採用 MDR 服務供應商，以補強、延伸，或外包其內部資安營運能力。

MDR 服務是一種由專家提供、全天候（24/7）全代管的資安服務，專門用來偵測與回應僅靠技術解決方案無法防範的網路攻擊。理想的 MDR 服務不僅會發出威脅警示，更能代表客戶執行完整的事件回應處置。透過結合人類專業知識與強大的防護技術、代理式 AI（Agentic AI）以及 AI 助手，資安分析師能夠偵測、調查並回應即使是最先進、由人類主導的攻擊行為，進而阻止勒索軟體、預防資料外洩，並避免營運中斷。MDR 不應與 EDR（端點偵測與回應）或 XDR（延伸式偵測與回應）混為一談。EDR 與 XDR 是工具，主要用來協助組織內部的資安營運團隊（若有的話）進行威脅調查、威脅獵捕與回應；而

MDR 則是讓組織借助資安服務供應商的專業團隊，包括分析師、威脅獵捕人員、研究人員與事件回應專家，代表客戶主動識別並消除威脅。

SOPHOS Managed Detection and Response (MDR) 託管式偵測與應變是由專家所提供的完全託管的服務，他們專責偵測與回應鎖定您電腦、伺服器、網路、雲端工作負載、電子郵件帳戶、備份等的網路攻擊。我們技術精湛的安全分析師團隊能夠阻止進階的人為攻擊，並迅速採取行動，在威脅影響您的業務營運或危害敏感資料前將其消除。

使用案例

1、24/7 全天候威脅監控

預期結果：透過專業人員代表您回應威脅的專家，以擴充您的 IT 和安全團隊。

解決方案：SOPHOS MDR 安全分析師會全天候監控、調查並回應威脅，執行即時的人為主導回應操作，以制止已確認的威脅。SOPHOS 僱有 500 多名威脅偵測與回應專家，並擁有七個全球安全營運中心的支援。

2、 加快威脅回應

預期結果：改善您對已確認威脅的平均回應時間 (MTTR)

解決方案：我們的分析師可以代表您執行威脅回應操作，以阻斷、封鎖和消除攻擊者，領先業界的平均威脅回應時間為 38 分鐘，比業界標準快 96%。

3、 攔截安全工具未能識別的威脅

預期結果：偵測出比安全工具自身能識別的更多的網路威脅。

解決方案：65% 的勒索軟體攻擊始於攻擊者利用合法使用者憑證或未知的弱點，而 29% 則始於被竊的憑證。SOPHOS MDR 分析師能進行主動的威脅捕獵，識別只有人類才能夠偵測到的攻擊者行為，並迅速消除僅靠工具無法阻止的威脅。

4、改善投資回報

預期結果：整合來自您的跨環境的安全解決方案，並從您的現有技術投資獲得更高的投資回報率 (ROI)。

解決方案：SOPHOS MDR 可以提供您所需的技術，或者充分利用您現有的網路安全投資，以偵測並回應威脅。SOPHOS 的開放式 AI 原生平台可收集、篩選並關聯來自各種網路安全與 IT 工具的資料，使 SOPHOS MDR 分析師能夠以更快的速度、更高的準確性和更透明的方式消除已確認的威脅。

SOPHOS MDR 包含以下防護內容：

- 24/7 專家主導的威脅監控和回應
- 包含 SOPHOS Endpoint 和 SOPHOS XDR 解決方案
- 監看 SOPHOS 防火牆
- 威脅事件發生期間直接聯絡客戶並協助處理
- 威脅回應：阻止並遏制主動攻擊
- 每週和每月報告

系統需求

安裝前工程師會與您確認設備系統版本，可使用版本如下：

<table>
<tr><th>產品</th><th colspan="3">系統需求</th></tr>
<tr><td>SOPHOS Central</td><td colspan="3">■ Microsoft Edge.
■ Google Chrome
■ Mozilla Firefox
■ Apple Safari (Mac only)</td></tr>
<tr><td rowspan="3">MDR Agent</td><td>支援平台</td><td>最少空間</td><td>最少記憶體</td></tr>
<tr><td>Windows Server 2016
Windows Server 2019
Windows Server 2022
Windows Server 2025</td><td>10 GB</td><td>8 GB</td></tr>
<tr><td>Amazon Linux 2
Amazon Linux 2023
CentOS Stream
Debian 11
Debian 12
Debian 13
Oracle 8
Oracle 9</td><td>2.5GB</td><td>2GB</td></tr>
</table>

	Oracle 10 RHEL 8 RHEL 9 RHEL 10 SUSE Linux Enterprise Server 15 Ubuntu 22.04 (LTS) Ubuntu 24.04 (LTS) 其餘 Linux 版本可參考官方網站： https://docs.SOPHOS.com/releasenotes/index.html?productGroupID=esg&productID=linux_protection&versionID=Agent		

Q&A:

Q1. 什麼是 MDR？與一般防毒軟體有何不同？

A1：

專家主導：MDR (Managed Detection and Response) 是由 SOPHOS 原廠專家團隊 24/7 全天候監控的受管服務。

主動處置：不同於防毒軟體僅能「被動偵測」，MDR 是由真人分析師主動獵捕潛在威脅。一旦發現攻擊跡象，專家會立即介入處置，將威脅消滅於萌芽階段。

Q2. 資安艦隊的「新 UTM 版」或「新旗艦版」提供的 MDR 服務內容為何？真的能幫企業省錢嗎？

A2：

專屬優惠：凡申辦 HiNet 資安艦隊 2026 系列「新 UTM 版」或「新旗艦版」，提供 SOPHOS MDR Essential Server 版一年訂閱服務，此服務市價每套高達 26,316 元，企業無需負擔高昂授權金與資安人才招聘成本，即可享有國際頂尖的 SOC（資安維運中心）等級防護。

- 「新 UTM-108 版」(SOPHOS XGS 108w) 提供一套 SOPHOS MDR Essential Server 版一年訂閱服務。
- 「新 UTM-128 版」或「新旗艦-128 版」(SOPHOS XGS 128w) 提供二套 SOPHOS MDR Essential Server 版一年訂閱服務。
- 「新 UTM-2100 版」或「新旗艦-2100 版」(SOPHOS XGS 2100) 提供三套 SOPHOS MDR Essential Server 版一年訂閱服務。
- 「新 UTM-3100 版」或「新旗艦-3100」(SOPHOS XGS 3100) 提供五套 SOPHOS MDR Essential Server 版一年訂閱服務。

Q3. 裝了 MDR 服務後，對企業有何實質好處與保障？

A3：

保護核心資產： 專為保護企業最關鍵的伺服器 (Server) 環境設計，防止其遭受勒索軟體或進階持續性威脅 (APT) 攻擊。

極大化減輕 IT 負擔： 企業不需自建大型 SOC 團隊，即可享有國際等級的 24 小時監控與專家即時響應服務。

Q4. 發生威脅時我需要自己處理嗎？

A4：

原廠直連處理：完全不需擔心。 當發現威脅時，SOPHOS 原廠專家團隊會直接代為處置 (如隔離受駭主機、切斷惡意連線)，無需客戶自行操作複雜介面或線上跟著原廠指示操作。

透明化報告： 威脅排除後，系統將提供一份摘要報告給企業端，詳述事件起因與處置結果，讓管理階層清晰掌握資安狀況，真正達到「安心託管」。

Q5. SOPHOS MDR 方案中包含 XDR 功能嗎？它如何與防火牆連動？

內含 XDR 技術： 本方案不僅提供專家服務，更內含 XDR (延伸偵測與回應) 端點防護產品。它能跨維度整合伺服器、網路與防火牆的資訊，讓潛伏的威脅無所遁形。

Active Threat Response：透過 XDR，MDR 專家可以實現與防火牆的主動連動。例如：當 XDR 偵測到伺服器有異常活動時，能指令防火牆立即主動阻斷該受駭設備的對外連線，防堵資料外洩。

整合優勢：「MDR+防火牆」的自動化協同作戰，能將原本需要數小時的人工判斷，縮短至秒級的自動化回應，確保威脅在擴散前就地正法，達成 1+1>2 的效果。