Sophos Managed Detection and Response

全天候威脅偵測和回應

Sophos MDR 是一項完全託管的 24/7 全天候服務，由專門偵測和回應鎖定電腦、伺服器、網路、雲端工作負載、電子郵件帳戶和其他網路攻擊的專家所提供。

勒索軟體和網路入侵防護服務

可始終運作的安全營運已成為當務之急。然而，當今作業環境複雜性高，網路威脅速度加快，使得大多數組織越來越難以自行偵測和進行回應。

透過 Sophos MDR，我們的專家團隊可以阻止進階的人為攻擊。我們會在網路威脅破壞您業務營運或危害敏感的資料前採取措施加以消除。Sophos MDR 為能針對不同的服務層進行客製，並可以透過我們的專有技術或您現有的網路安全技術來實施。

以服務形式提供網路安全

Sophos MDR 透過擴展式偵測和回應 (XDR) 功能提供完整的安全保護。無論資料位於何處，都可以：

- **偵測出安全工具疏漏的更多網路威脅**
  我們的工具會自動阻擋 99.98% 的威脅，讓我們的分析師能夠專注於捕獵最複雜的攻擊者。只有訓練有素的專家可以偵測和阻擋這類威脅。
- **為您採取行動防止威脅影響業務**
  我們的分析師可以在幾分鐘內偵測、調查和回應威脅——無論您需要的是全面事件回應還是幫助做出準確的決策。
- **找出威脅的根本原因以防未來發生的事件**
  我們會主動採取措施並提供降低風險的建議。事件減少，您的 IT 和安全團隊、員工和客戶受到的干擾也會更少。

與現有的網路安全工具相容

我們可以從我們屢獲殊榮的產品組合中提供您所需的技術，或者，我們的分析師也可以使用您現有的網路安全技術來偵測和回應威脅。

Sophos MDR 與 Microsoft、CrowdStrike、Palo Alto Networks、Fortinet、Check Point、Rapid7、Amazon Web Services (AWS)、Google、Okta、Darktrace 等廠商的安全遙測來源相容。這些遙測來源可以自動與來自 Sophos 自適應生態系統 (ACE) 和 Sophos X-Ops 威脅情報部門的深入資訊整合、進行關聯並確定優先等級。

產品重點

- 透過一組 24/7 全天候威脅回應專家團隊來阻止勒索軟體和其他人為主導的進階型攻擊
- 完全發揮現有網路安全技術的投資回報
- 讓 Sophos MDR 進行全面的事件回應、與您一起管理安全事件，或是提供詳細的威脅通知和指引
- 透過 24/7 全天候監控和端點偵測與回應 (EDR) 功能提高網路保險理賠範圍
- 減輕內部 IT 和安全人員的負擔，使他們能專注於業務支援

SOPHOS

滿足您處境所需的 MDR

Sophos MDR 能客製化，提供不同的服務等級和威脅回應選項。您可以讓 Sophos MDR 營運團隊執行全面的事件回應、與您一同管理網路威脅，或是在偵測到威脅時通知您的內部安全營運團隊。我們的團隊可以快速了解攻擊的對象、內容、時間和方式，並可以在幾分鐘內對威脅做出反應。

主要功能

24/7 全天候威脅監控和回應

我們會在威脅危害您的資料或導致停機之前就先行偵測出來並做出回應。Sophos MDR 提供全天候服務，以六個全球安全營運中心 (SOC) 進行支援。

相容於非 Sophos 的安全工具

Sophos MDR 可以將來自第三方端點、防火牆、身分識別、電子郵件和其他安全技術的遙測整合為 Sophos ACE 的一部分。

全面的事件回應

當我們發現一個主動的威脅時，Sophos MDR 營運團隊可以為您執行一系列的回應，包括遠端破壞、遏阻和徹底消滅對手。

提供每週和每月報告

Sophos Central 是用於即時警示、報告和管理的單一儀表板。每週和每月報告將提供安全調查、網路威脅和現在安全狀況的深入資訊。

Sophos 自適應網路安全生態系統

Sophos ACE 能自動阻止惡意活動，讓我們能夠尋找弱訊號以發現需要人工介入才能偵測、調查和消除的威脅。

由專家主導的威脅捕獵

由訓練有素的分析師進行的主動威脅捕獵，可發現並迅速消除安全產品本身無法偵測到的威脅。Sophos MDR 營運團隊還可以使用第三方廠商遙測來進行威脅捕獵，並識別出躲避現有部署工具偵測的攻擊者行為。

直接通話支援

您的團隊可以直接致電我們的安全營運中心 (SOC)，以查看潛在威脅和進行中的事件。Sophos MDR 營運團隊 24/7/365 全天候提供服務，並由遍布全球 26 個地點的支援團隊提供支援。

專屬的事件回應負責人

我們會為您提供專門的事件回應負責人。一旦發現事件，他會與您的內部團隊和外部合作夥伴協作，直到事件解決。

根本原因分析

除了提供主動建議以改善安全狀況外，我們還會執行根本原因分析，以確定導致事件的潛在問題。我們為您提供建議性指引來解決安全漏洞，防止它們在未來遭到利用。

Sophos 帳戶健康情況檢查

我們不斷檢視 Sophos XDR 管理端點的設定和配置，並確保它們以最高效率運作。

威脅遏阻

如果組織選擇不用 Sophos MDR 進行全面事件回應，那麼 Sophos MDR 營運團隊可以採取威脅遏阻措施，中斷威脅並防止擴散。如此一來可以減輕內部安全營運團隊的工作，讓他們能夠快速進行補救措施。

情報簡報：“Sophos MDR ThreatCast”

由 Sophos MDR 營運團隊提供的 “Sophos MDR ThreatCast” 是專為 Sophos MDR 客戶提供的每月簡報。這份簡報將提供最新威脅情報和安全最佳作法的深入資訊。

Sophos 服務層級

	Sophos Threat Advisor	Sophos MDR:	Sophos MDR Complete
24/7 全天候由專家主導的威脅監控和回應	✓	✓	✓
與非 Sophos 安全產品相容	✓	✓	✓
每週和每月報告	✓	✓	✓
每月情報簡報：“Sophos MDR ThreatCast”	✓	✓	✓
Sophos 帳戶健康情況檢查		✓	✓
由專家主導的威脅捕獵		✓	✓
威脅遏阻：中斷攻擊、防止擴散 使用完整的 Sophos XDR 代理程式 (保護、偵測和回應) 或 Sophos XDR Sensor (偵測和回應)		✓	✓
事件期間的直接電話支援		✓	✓
全面的事件回應：完全消除威脅 需要完整的 Sophos XDR 代理程式 (保護、偵測和回應)			✓
根本原因分析			✓
專屬的事件回應負責人			✓

免費包含整合功能

可以免費整合來自以下來源的安全資料，以供 Sophos MDR 營運團隊使用。遙測來源可用於擴展整個環境的可見性、產生新的威脅偵測項目並提高現有威脅偵測的保真度、進行威脅捕獵，以及啟用額外的回應功能。

Sophos XDR

唯一結合原生的端點、服務器、防火牆、雲端、電子郵件、行動和 Microsoft 整合功能的 XDR 平台

Sophos Firewall

監控和篩選傳入和傳出的網路流量，在進階型威脅有機會造成傷害之前加以阻止

Microsoft Graph 安全性

- 適用於端點的 Microsoft Defender
- 適用於雲端的 Microsoft Defender
- 適用於身分識別的 Microsoft Defender
- Azure Active Directory
- 適用於雲端應用程式的 Microsoft Defender
- Microsoft Sentinel
- Azure 資訊保護
- Microsoft 365

Sophos 端點

阻止進階型威脅並偵測惡意行為——包括模仿合法使用者的攻擊者

Sophos 網路偵測和回應

持續監控網路內的活動，偵測出裝置之間原本無法發現的可疑行為

第三方端點保護

相容於

- Microsoft
- Crowdstrike
- SentinelOne
- Check Point
- Trend Micro
- BlackBerry (Cylance)
- McAfee
- Malwarebytes

Sophos Cloud

防止雲端資料外洩並取得關鍵雲端服務的可見性，包括 AWS、Azure 和 Google Cloud Platform

Sophos Email

保護收件夾免受惡意軟體的危害，並使用進階型 AI 防範針對性的身分假冒和網路釣魚攻擊

90 天資料保留

Sophos MDR 服務中包含 Sophos XDR 和 Sophos Endpoint Protection 產品
在與 Sophos MDR 服務整合之前，必須購買和部署 Sophos Firewall、Sophos Cloud、Sophos Email 和 Sophos NDR 產品

附加整合功能

透過購買整合功能套件，可以整合來自以下第三方來源的安全資料，以供 Sophos MDR 營運團隊使用。遙測來源可用於擴展整個環境的可見性、產生新的威脅偵測項目並提高現有威脅偵測的保真度、進行威脅捕獵，以及啟用額外的回應功能。

Firewall

相容於

- Palo Alto Networks
- Fortinet
- Check Point
- Cisco
- SonicWall

雲端

相容於

- AWS
- Microsoft Azure
- Orca Security
- Google Cloud

身分識別

相容於

- Okta
- Duo

網路安全性

相容於

- Darktrace
- Forcepoint
- McAfee (Web Gateway)

電子郵件

相容於

- Proofpoint
- Mimecast

1 年資料保留

Sophos MDR 的 Onboarding Plus 套件

我們的 Onboarding Plus 產品組合是一項提供給 Sophos MDR 客戶的遠端引導式上線服務。該服務讓您可以聯繫 Sophos 專業服務組織內的專屬聯繫人，以獲得產品上線和安排、部署和培訓的協助以及健康狀況檢查，確保您可以經由我們的最佳作法獲得最大價值。Onboarding Plus 包括：

第 1 天 — 實作計畫和執行：

- 啟動專案。
- 設定 Sophos Central
- 檢視 Sophos Central 的功能
- 建立和測試部署程序
- 在您的組織中部署 Sophos Central

第 30 天 — XDR 培訓

- 學習如何像 SOC 一樣思考和行動
- 尋找入侵指標 (IOC)
- 為未來的調查建立查詢

第 90 天 — XDR 培訓

- 檢視您目前的安全政策，並依需要進行更新。
- 確認可使用哪些功能 (如有) 進一步增強您的網路保護
- 收到包含我們健康狀況檢查建議的書面文件

如需了解更多資訊，請瀏覽：

sophos.com/mdr

台灣業務窗口
電子郵件：Sales.Taiwan@Sophos.com

22-10-17 DS-ZHTW (DD)

SOPHOS