解決方案手冊

Sophos Extended Detection and Response

使用 AI 驅動的 EDR 和 XDR 防衛主動攻擊敵手

迅速阻止攻擊至關重要。Sophos 開放式的 AI 原生 XDR 平台提供強大的工具和威脅情報，使您能夠在您的整個 IT 環境中偵測、調查和回應可疑活動。

建立在最強大的保護基礎上

當更多威脅能提前被阻擋，資源緊迫的 IT 團隊需要調查和解決的事件就能減少。Sophos 將擴展式偵測和回應技術與業界最強大的端點防護相結合，在需要手動調查之前即可阻擋威脅，減輕您的工作負擔。

內建端點偵測與回應 (EDR)

Sophos XDR 包含全面的 EDR 工具，其中包括強大且可自訂的搜尋功能，能夠存取長達 90 天的豐富端點和伺服器資料 (標準功能)，並支持對您裝置的安全遠端存取。調查問題、安裝和解除安裝軟體，終止處理程序等。

透過生成式人工智慧 (GenAI) 加速安全營運

Sophos XDR 中廣泛的生成式人工智慧能力可賦予團隊做出明智決策的能力，進而提升分析師的信心與企業的信心。Sophos AI Assistant 助手能夠引導不同技術水平的使用者完成威脅調查的每個階段，使您能夠迅速應對並消除敵手威脅。

將可見性擴展到端點之外

您能看到的越多，越能快速行動。您將可以擷取、篩選、關聯 Sophos 和非 Sophos 產品的事件並進行排優先序，擴展所有關鍵受攻擊面的可見性，讓您能夠快速偵測並阻擋主動攻擊者。Sophos XDR 與您現有的工具和技術相容，其整合功能涵蓋身分識別、網路、防火牆、電子郵件、雲端、生產力工具、備份以及端點安全解決方案。

廣泛的 Sophos XDR 就緒的解決方案

各種 Sophos 技術可在 XDR 平台中無縫協作，提供最佳的安全成效。原生解決方案整合包括 Sophos Endpoint、Sophos Workload Protection、Sophos Mobile、Sophos Firewall、Sophos NDR、Sophos ZTNA、Sophos Email 和 Sophos Cloud Optix。

產品重點

- 獲得所有關鍵受攻擊面上可疑活動的可見性
- 一個整合多種解決方案的開放式 XDR 平台
- 利用現有的工具和投資，整合廣泛的非 Sophos 技術來提升效益
- 透過排優先序的偵測和人工智慧驅動的工具，快速調查並回應威脅
- 包含業界領先的端點防護和 EDR 功能

以最高效率進行偵測、調查與回應

Sophos XDR 包含專為提升安全分析師和 IT 管理員效率而設計的工具與工作流程。自動生成的案件讓您能夠快速調查潛在威脅，了解事件的範圍和原因，並最大限度縮短回應的時間。

涵蓋所有主要受攻擊面的 AI 優先排序偵測

輕鬆識別需要立即關注的可疑活動 Sophos XDR 會根據風險自動排優先序偵測，且提供完整的相關資訊。

MITRE ATT&CK 架構對應

可自動將偵測和個案對應到 MITRE ATT&CK Tactics，使您能夠輕鬆找出防禦上的漏洞並優先改進。

快速調查和捕獵威脅

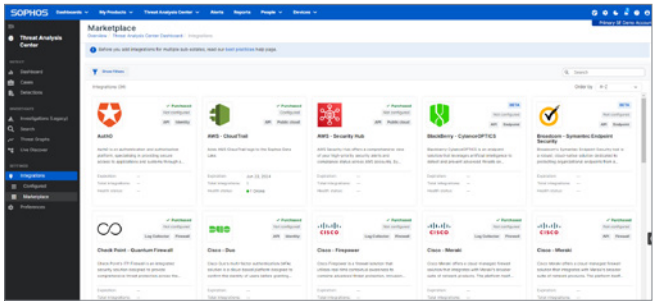
提供強大的搜尋工具，包括預先設置的查詢範本，可讓您無需成為 SQL 專家也可更快地找到所需的資料。

自動化和加速的回應

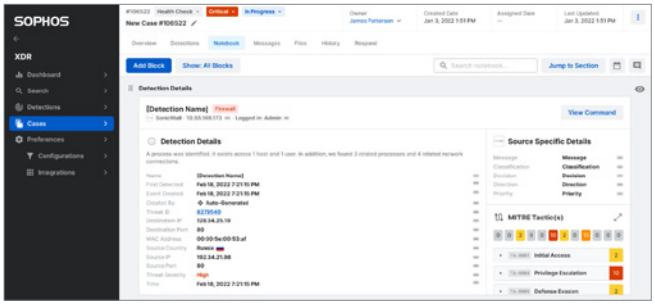
提供自動化的行動，如處理程序終止、勒索軟體回復和網路隔離等，能快速封鎖威脅，並節省您寶貴的時間。

協作式個案管理

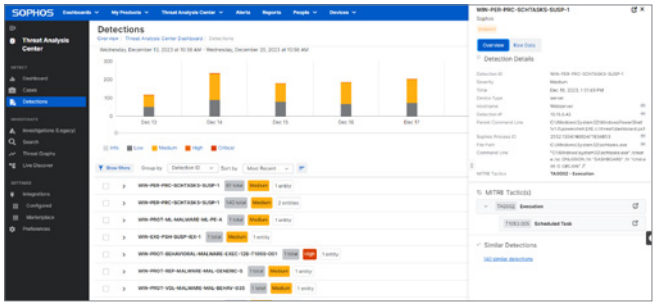
自動個案建立功能可實現快速調查，並提供全面的個案管理工具 以便與其他團隊成員進行協作。



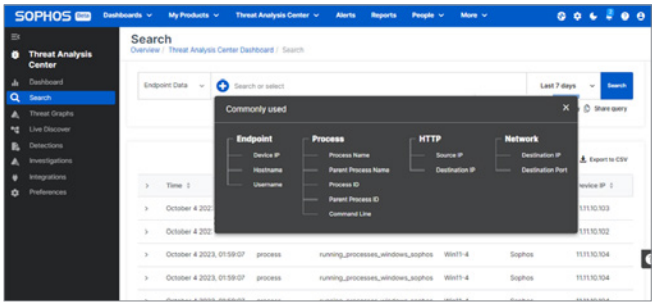
相容於 Sophos 和第三方解決方案



強大的個案管理和協作工具



AI 排優先序的偵測能涵蓋所有主要的受攻擊面



簡單而強大的搜尋——無需 SQL 專業知識

透過 GenAI 加速安全營運

Sophos XDR 中廣泛的生成式人工智慧能力，賦予您的團隊做出明智決策並更快消除威脅的能力，從而提升分析師的信心與企業的信心。GenAI 功能是可選的，讓您擁有完全的控制權。

AI Assistant

能夠引導不同技術水平的使用者完成威脅調查的每個階段，發揮最大效率以快速阻擋威脅。

AI 搜尋

採用自然語言搜尋功能加速日常工作，並降低安全營運的技術門檻。

AI 案件摘要

提供易於理解的偵測概覽和建議的下一步行動，可幫助分析師快速做出明智決策。

AI 指令分析

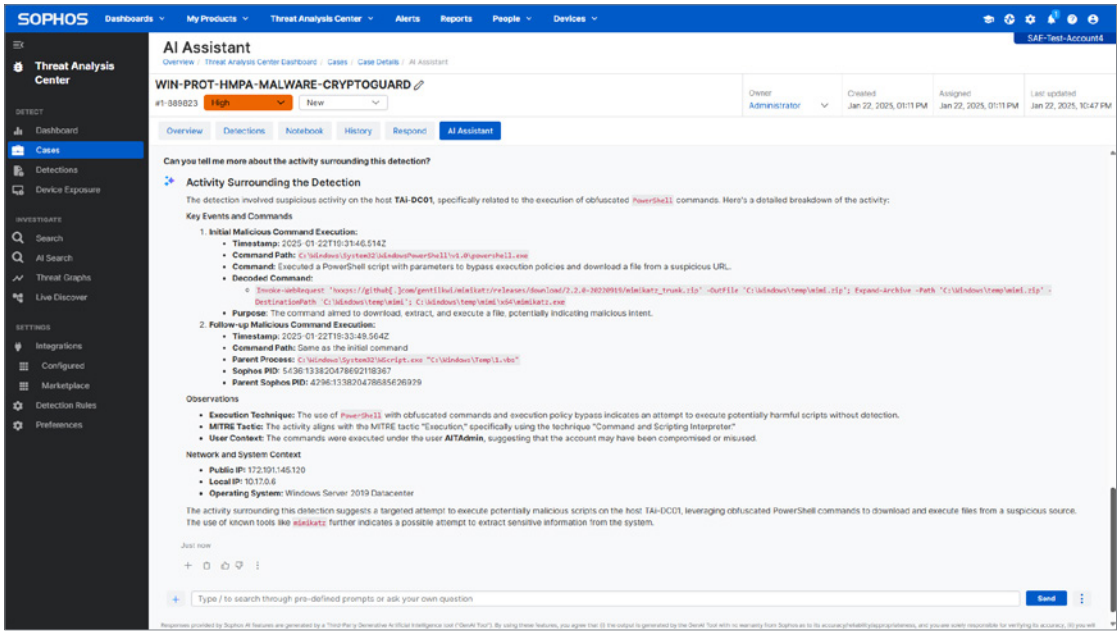
分析複雜的命令列參數，揭示其目的與影響，並以淺顯易懂的語言加以解釋。

Sophos AI Assistant

Sophos AI Assistant 讓所有使用者——從一般 IT 人員到 Tier 3 SOC 分析師——都能輕鬆獲取所需資訊，以推動威脅調查並迅速遏阻攻擊敵手。

- **執行各種廣泛的安全營運任務：**分析可疑指令、分析可疑指令、列出入侵指標 (IOC)、利用威脅情報強化數據、創建詳細報告等。
- **與 Sophos 一線安全分析師作合設計：**受益於真實世界的工作流程和 Sophos MDR 專家的經驗。
- **可使用日常語言提問，或選擇 Sophos 威脅專家提供的預設提示。**獲得清晰的摘要與建議的後續步驟。
- **根據威脅態勢持續更新：**確保可獲取來自 Sophos X-Ops 的最新調查技術和威脅情報。

這不只是另一個 AI 工具，而是來自全球領先的託管式偵測與回應 (MDR) 服務團隊的專業知識，並淬煉為一個智慧型代理程式。



Sophos XDR 包含許多整合功能

無需額外成本把把以下來源的安全資料和 Sophos XDR 平台整合。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。

Ep Sophos Endpoint

阻擋進階型威脅並偵測跨端點上的惡意行為

Sophos XDR 定價中包含的產品

WP Workload Protection

針對 Windows 和 Linux 伺服器以及容器的進階防護和威脅偵測

Sophos XDR 定價中包含的產品

Mob Sophos Mobile

確保您的 iOS 和 Android 裝置以及資料免受最新的行動威脅的侵害

產品單獨出售；無需額外費用即可整合

Fw 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

產品單獨銷售；需要有 XStream Protection 訂購；集成無需額外收費

Em Sophos Email

保護收件匣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

產品單獨銷售；需要有 XStream Protection 訂閱；集成無需額外收費

Cld Sophos Cloud Optix

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 (GCP)

產品單獨出售；無需額外費用即可整合

ZT Sophos ZTNA

以最小權限存取來取代遠端存取 VPN，來安全地將使用者連線到您的網路應用程式

產品單獨出售；無需額外費用即可整合

第三方端點防護

整合包括：

- Broadcom Symantec
- CrowdStrike
- Cylance
- Jamf
- Microsoft
- SentinelOne
- Trend Micro

使用 Sophos XDR Sensor 代理程式，與其他端點防護解決方案相容

Microsoft 安全工具

- Defender for Endpoint
- Defender for Office 365
- Microsoft Defender for Cloud Apps
- Defender for Identity
- Entra ID Protection
- Microsoft 365 Defender
- Microsoft PurView DLP

90 天資料保留

標準為偵測資料在 Sophos 資料湖中可保留長達 90 天。

Microsoft Office 365 Management Activity

提供來自 Office 365 Management Activity API 擷取的使用者、管理員、系統、政策動作和事件資訊

Google Workspace

從 Google Workspace Alert Center API 中擷取的安全遙測資訊

附加整合功能

可購買 Integration Packs 整合套件以整合來自以下來源的安全資料，以供 Sophos XDR 平台使用。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 NDR

持續監控網路內的活動，偵測出原本無法發現的裝置之間發生的可疑行動

透過 SPAN 連接埠鏡像與任何網路相容

防火牆

整合包括：

- Barracuda
- Check Point
- Cisco Firepower
- Cisco Meraki
- Fortinet
- F5
- Forcepoint
- Palo Alto Networks
- SonicWall
- Ubiquiti
- WatchGuard

網路

整合包括：

- Cisco Umbrella
- Darktrace
- Secutec
- Skyhigh Security
- Thinkst Canary
- Vectra
- Zscaler

身分識別

整合包括：

- Auth0
- Cisco ISE
- Duo
- ManageEngine
- Okta

已免費包含 Microsoft 整合功能

電子郵件

整合包括：

- Mimecast
- Proofpoint
- Trend Micro

無需額外成本已包含 Microsoft 365 和 Google Workspace 整合功能

雲端平台

整合包括：

- Orca Security

AWS，Azure 和 GCP 集成隨 Sophos Cloud Optix 產品提供，單獨銷售。

備份與復原

整合包括：

- Acronis
- Rubrik
- Veeam

1 年資料保留

標準情況下，將偵測資料保留在 Sophos 資料湖中一年。

建立在全球最佳端點防護基礎上

在駭侵發生之前就加以阻止，讓您專注於調查。大多數 XDR 產品會迫使分析師浪費寶貴的時間來調查應該已經被防護方案擋住的事件。Sophos 將 XDR 與業界最強大的端點防護相結合，在需要手動調查之前即可阻擋威脅，減輕您的工作負擔。

Sophos XDR 訂閱包括 Sophos Endpoint，提供先進的反勒索軟體和反漏洞利用防護、AI 驅動的惡意軟體防護，以及能根據主動攻擊動態來提升保護層級的自適應防禦。

了解更多資訊：www.sophos.com/endpoint

以完全託管的服務形式取得偵測與回應能力

您可以選擇使用 Sophos XDR 自行偵測和調查威脅，或者使用全方位的 24/7 全天候託管服務節省員工的時間。透過 Sophos Managed Detection and Response (MDR)，我們的威脅捕獵專家和分析師團隊可以為您提供一個即時的安全營運中心，包括全面的事件回應能力。

了解更多資訊：www.sophos.com/mdr

隨附於 Sophos XDR 訂閱中

	Sophos XDR
AI 生成的威脅評分和排優先級的偵測	✓
個案管理、協作和回應行動	✓
提供簡單而強大的搜尋工具以用於捕獵和調查	✓
由 GenAI 驅動的 XDR 功能 (選用)： AI Assistant、AI 案件摘要、AI 指令分析、AI 搜尋	✓
Sophos Endpoint 和 Workload Protection 解決方案	✓
端點偵測與回應 (EDR) 工具	✓
將偵測資料保留在 Sophos 資料湖中 (標準為 90 天)	✓
可用於 EDR 的端點和伺服器裝置內資料	✓
與 Sophos 解決方案整合： Sophos Endpoint、Sophos Workload Protection、Sophos Mobile、 Sophos Firewall、Sophos ZTNA、Sophos Email、Sophos Cloud Optix	✓
Sophos Network Detection and Response (NDR)	可選附加功能
與非 Sophos 端點保護解決方案的整合	✓
與 Microsoft 解決方案的整合	✓
與 Google Workspace 生產力解決方案的整合	✓
與非 Sophos 防火牆、網路、電子郵件、雲端、身分識別，以及備份和復原解決方案的整合	可選附加功能

客戶為何選擇 Sophos XDR

Sophos 是擁有業界認可的擴展式偵測與回應的領先者。

Gartner

Sophos 在 2024 年Gartner 端點保護平台®魔力象限™ 評比中連續 15 次獲評為領導者之一

Gartner Peer Insights Customers' Choice 2024

Sophos 獲評為 2024 年 Gartner®Peer Insights™ 端點防護平台和網路防火牆的客戶首選

G2 Leader

Sophos 在 2025 年冬季 G2 Grid® 報告中獲評為端點防護、EDR、XDR、防火牆和 MDR 的領導者之一

MITRE | ATT&CK® Evaluations

Sophos 在 2024 年 MITRE Engenuity ATT&CK Evaluations: Enterprise for EDR/XDR solutions 中取得優異成績

SE Labs

Sophos 在 SE Labs 獨立安全測試中持續取得業界領先的保護成績

立即免費試用

註冊取得 30 天免費試用
www.sophos.com/xdr

台灣業務窗口
電子郵件：Sales.Taiwan@Sophos.com

2025-02-10 DS-ZHTW (PS)

SOPHOS