

解決方案簡介

# Sophos XDR

## 使用 EDR 和 XDR 防衛主動攻擊敵手



攻擊敵手不斷改進他們的技術，利用各種漏洞並加快攻擊的時間表。縮短偵測和回應的時間從未如此重要。Sophos 的統一擴展式偵測與回應 (XDR) 平台能夠在您整個安全生態系統中快速偵測、調查和回應多階段威脅和主動攻擊敵手。

### 使用案例

#### 1 | 從強大的防禦開始

**預期結果:**預先阻止更多威脅，以減輕您的工作量。

**解決方案:**將調查的重點放在駭侵發生之前就加以阻止。Sophos XDR 包括無與倫比的保護，能夠在進階型威脅升級前就加以迅速阻止。使用先進技術，包括人工智慧、行為分析、防勒索軟體和防漏洞利用等，來保護端點和伺服器。

#### 2 | 加快威脅回應

**預期結果:**快速偵測、調查並回應威脅。

**解決方案:**利用 Sophos X-Ops 的威脅情報，透過 AI 安排優先順序的偵測讓您能快速且輕鬆地辨識出需要立即關注的可疑事件。進行威脅捕獵，並以最佳化的調查工作流程、強大的搜尋功能、案件管理協作工具和自動化回應，快速做出反應。

#### 3 | 受攻擊面的可見性

**預期結果:**獲得所有主要受攻擊面上具規避能力的威脅的完整可見性和洞察力。

**解決方案:**使用 Sophos 全面整合和 XDR 就緒的解決方案，提供超越端點的可見性，或是發揮您現有的技術投資。將第三方端點、防火牆、網路、電子郵件、身分識別和雲端安全解決方案的廣泛生態系統整合，利用統一的 XDR 平台來偵測並回應威脅。

#### 4 | 適用於所有使用者的強大功能

**預期結果:**一般 IT 人員和安全分析人員都可以輕鬆進行調查和回應。

**解決方案:**Sophos XDR 設計給專門的內部 SOC 團隊和負責安全及其他 IT 工作的系統管理員使用，有助於完全發揮使用者效率，提供協助您回應威脅的完整可見性和指導。

**Gartner**

在 2023 年 Gartner XDR 市場指南中受到肯定

**MITRE  
ATT&CK**

在 2023 年 MITRE Engenuity ATT&CK 評估中取得優異成績

**G2 Leader**

獲 G2 使用者評價為第一的 XDR 解決方案 (2023 年春季)

了解更多資訊並進行試用

**Sophos XDR:**  
[sophos.com/xdr](https://sophos.com/xdr)