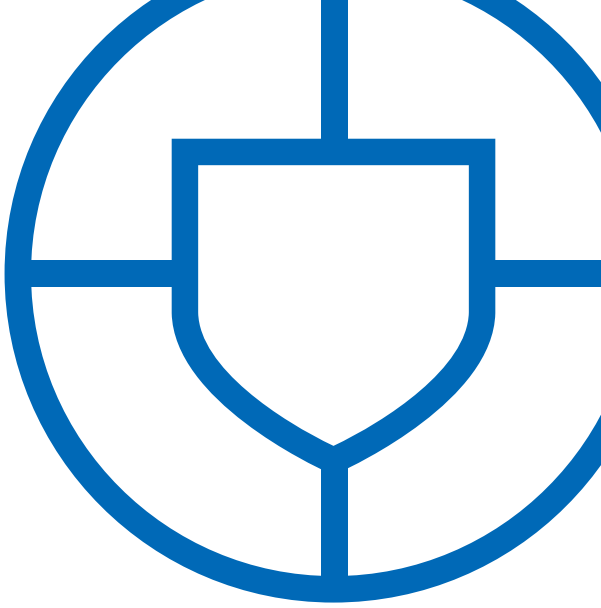
SOPHOS

Cybersecurity made simple.



端點安全購買指南

隨著網路威脅變得越來越複雜，IT和安全管理員取得適當端點解決方案的壓力也越來越大。然而，端點安全市場中充斥著各種不同的解決方案，並且滿是難以辯駁的行銷觀點，因此為您的組織做出明智決策變得越來越困難。

我們面臨的威脅及防範技術快速變化，已造成普遍的混亂。本指南將帶您清楚了解重要的防範技術，確保您的端點具備保護組織所需的適當防禦。此外，您也可以了解不同廠商在獨立測試中的結果，協助您做出明智的選擇。

您並不孤單

不知道應該如何端點安全解決方案？擔心自己沒有適當的保護？您並不孤單。以下是其他 IT 與資安專家的說法[1]：

- 87% 同意惡意軟體威脅在去年變得越來越複雜
- 60% 認為他們目前的網路防禦不足以阻擋現今網路威脅
- 60% 打算在未來 12 個月內實作機器學習
- 56% 不了解機器學習與深度學習之間的差異
- 46% 宣稱自己已經擁有防入侵攻擊技術 – 但有 2/3 的人實際上不了解防入侵攻擊技術是什麼

如此看來，許多人不清楚什麼是端點安全一點也不奇怪。本指南的目的是協助您做出明智選擇，並為貴組織設置最佳的保護。

產品特色和功能

端點安全解決方案(有時簡稱為防毒解決方案)可包括各種用來防範端點威脅的基本(傳統)和現代(新一代)方法。評估解決方案時，重要的是要尋找具備全方位技術，可阻擋各種威脅的解決方案。此外，了解您試圖防禦的威脅也很重要。

端點威脅

雖然威脅情況持續不斷變化，但以下是在評估不同解決方案時應該考慮的一些重要端點威脅：

- **可攜式執行檔 (惡意軟體)：**考量端點保護時，首要考慮的往往是惡意軟體程式 (惡意軟體)。惡意軟體包括已知和從未見過的惡意軟體。一般來說，解決方案都難以偵測未知的惡意軟體。這很重要，因為 SophosLabs 每天都會看到大約四十萬個未知的惡意軟體。解決方案應該善於發現已遭修改使其難以辨識的封裝與多型態檔案。
- **可能不需要的應用程式 (PUA)：**技術上來說，PUA 不是惡意軟體，但很可能是您不想在電腦上執行的應用程式 (例如廣告軟體)。隨著加密劫持攻擊中使用的加密貨幣挖礦程式越來越多，PUA 偵測也越來越重要。
- **勒索軟體：**在過去一年中，超過一半的組織都曾遭到勒索軟體攻擊，平均花費 133,000 美元[2]。勒索程式的兩大主要類型為檔案加密與磁碟加密 (抹除器)。檔案加密最常見，它會加密並挾持受害者的檔案以便索取贖金。磁碟加密會鎖定受害者的整個硬碟 (不只是檔案)，或將硬碟整個抹除。
- **入侵攻擊型與無檔案型攻擊：**並非所有攻擊都依賴惡意軟體。入侵攻擊型攻擊使用利用軟體錯誤與弱點的技術，以便取得您電腦的存取權與控制權。武器化文件 (通常是經過加工或修改以造成損害的 Microsoft Office 程式) 和惡意指令碼 (惡意程式碼常常隱藏在合法程式與網站中) 是這些攻擊所使用的常見技術類型。其他範例包括瀏覽器中間人攻擊 (使用惡意軟體感染瀏覽器，讓攻擊者得以檢視與操控流量) 和惡意流量 (使用網頁流量進行邪惡目的，例如聯繫命令與控制伺服器)。
- **主動攻擊技術：**許多端點攻擊都包含多個階段與多個技術。主動攻擊技術的範例包括權限提升 (攻擊者用來取得系統額外存取權的方法)、認證竊盜 (竊取使用者名稱與密碼)，以及程式碼洞穴 (將惡意程式碼隱藏在合法應用程式中)。

現代 (新一代) 技術與基本 (傳統) 技術

雖然防毒解決方案的名稱可能不同，不過它已經存在一段時日，而且證明其防禦已知威脅很有效。傳統端點保護解決方案必須使用各式各樣的基本技術。不過，隨著威脅情況改變，未知威脅 (例如從未見過的惡意軟體) 已變得越來越常見。因此，新技術也已在市場上出現。購買者應該尋找結合現代方法 (常稱為「新一代」安全性) 與經驗證的基本作法的解決方案。部分重要功能包括：

基本功能

- **防惡意軟體/防毒：**已知惡意軟體的特徵碼型偵測。惡意軟體引擎應該不只有能力檢查執行檔，也要能檢查其他程式碼，例如網站上發現的惡意 JavaScript。
- **應用程式鎖定：**阻止應用程式的惡意行為，例如會安裝其他應用程式並加以執行的武器化 Office 文件。
- **行為監控/主機型入侵防禦系統 (HIPS)：**這個基本技術可保護電腦免於未辨識病毒與可疑行為的攻擊。它應該包含執行前與執行階段行為分析。
- **網頁保護：**URL 查詢和阻擋已知惡意網站。遭阻擋的網站應該包含可能執行 JavaScript 以進行加密貨幣挖礦的網站，以及獲取使用者驗證認證與其他敏感資料的網站。
- **網頁控制:**端點網頁篩選可讓系統管理員定義使用者可從網際網路下載哪些檔案類型。
- **資料遺失防禦 (DLP)：**如果攻擊躲過監控，DLP 能夠偵測及防止某些攻擊的最後階段 (也就是攻擊者嘗試竊取資料時)。這項功能透過監控各種敏感資料類型而達成的。

現代功能:

- **機器學習：**機器學習方法的類型有很多種，包括深度學習神經網路、隨機森林、貝氏和叢集。不論使用何種方法，機器學習惡意軟體偵測引擎都應該能偵測已知與未知的惡意軟體，而不依靠特徵碼。機器學習的優點在於，它可以偵測從未見過的惡意軟體，理想情況下能提升整體惡意軟體偵測率。組織應該評估機器學習型解決方案的偵測率、誤報率和效能影響。
- **防入侵攻擊：**防入侵攻擊技術是透過防範攻擊者在攻擊鏈中使用的工具與技術來進行防禦。例如，EternalBlue 與 DoublePulsar 等入侵攻擊是用來執行 NotPetya 與 WannaCry 勒索軟體。防入侵攻擊技術可阻擋用來散播惡意軟體與執行攻擊的某些技術而不需要事先看過它們，因此能抵禦許多零時差攻擊。
- **勒索軟體專用：**有些解決方案是專為防範勒索軟體對檔案惡意加密而設計的。勒索軟體專屬技術通常也會修復受影響的檔案。勒索軟體解決方案不應只是阻止檔案勒索軟體，還要阻止會竄改主要開機記錄的破壞性抹除器攻擊中所使用的磁碟勒索軟體。
- **認證竊盜防護:** 防止從記憶體、登錄檔偷竊驗證密碼和雜湊資訊，以及關閉硬碟。
- **處理序保護 (權限提升)：** 這種保護的設計是判斷高權限的驗證權杖何時插入處理序以提升權限。無論使用哪種已知或未知的弱點來竊取驗證權杖，這項功能都能發揮作用。
- **處理序保護 (程式碼洞穴)：**防止使用如程式碼洞穴和 AtomBombing 的技術。惡意份子經常使用這類技術利用現有的合法應用程式。惡意份子會濫用這些呼叫，讓其他處理序執行其程式碼。
- **端點偵測與回應 (EDR)/根本原因分析：**EDR 和其他分析工具並不專注於防範攻擊，而是分析及回應之前偵測到的事件。有些也會提供追捕功能，以發現過去未曾注意到的攻擊。重要的是，您應該考慮工具的複雜性與易用性必須符合 IT 團隊的規模和技術能力。
- **事件回應/同步安全性：** 端點工具最少應該提供已發生事件的深入資訊，協助避免未來的事件。理想上，它們應自動回應事件，無需分析人員介入，以阻止威脅擴散或造成更多損害。重要的是，事件回應工具要能與其他端點及網路安全工具溝通。

「合體的力量」：結合多種技術，實現全方位的端點安全。

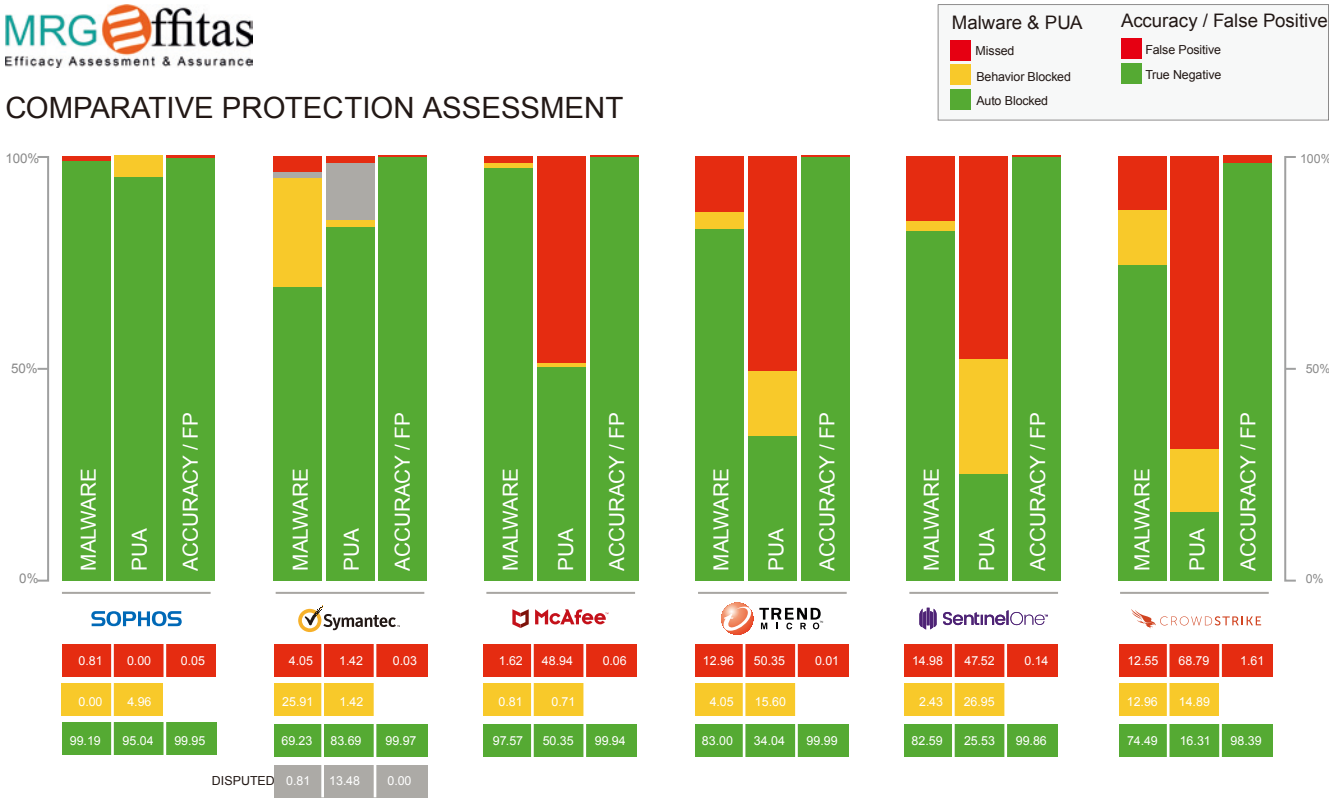
評估端點解決方案時，組織不應只看一個主要功能。反之，應該尋找一系列令人印象深刻的功能，包括現代技術 (例如機器學習) 和經過驗證依然有效的基本方法。如果仰賴單一主要功能，即使是它已經是同級最佳，仍意味著容易出現單一失敗點的情形。反之，深度防禦方式 (多個強大安全層的組合) 將可阻擋較廣泛的威脅。這就是我們常說的「合體的力量」：結合基本技術、機器學習、防入侵攻擊、防勒索軟體，再加上其他更多功能。評估端點安全時，一定要記得詢問各廠商他們的解決方案內包含哪些技術。各元件的優點為何？它們是設計來阻擋哪些威脅的？它們是否仰賴單一主要技術？如果失敗了，該怎麼辦？

Sophos 與競爭對手的比較

比較擁有不同功能的產品已經很困難，若要比較它們在模擬遭受攻擊者無限多種且未知的攻擊時的效能，更加是不可能的。想要自行測試的使用者，可以在此處找到一份介紹性的測試指南。不過，許多組織選擇仰賴第三方評估來協助他們做出採購決策。

MRG Effitas 惡意軟體防護測試

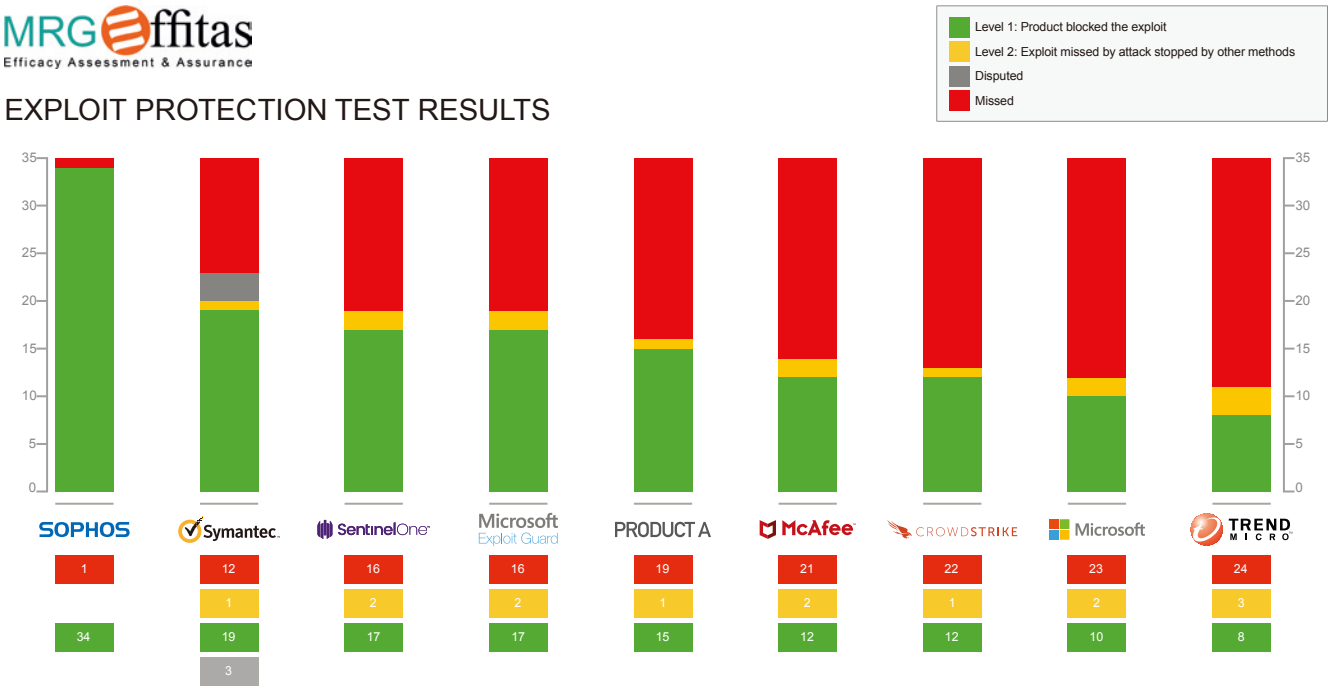
MRG Effitas 接受委託進行了一項測試，比較不同端點保護產品偵測惡意軟體與可能不需要的應用程式 (PUA) 的能力。測試中審查了六個不同廠商，包括 Sophos 在內。Sophos 在偵測惡意軟體中排名第一，在偵測可能不需要的應用程式中也排名第一。Sophos 還具備令人印象深刻的誤報率。



請到此處閱讀完整結果。

MRG Effitas 入侵攻擊與入侵攻擊後防護測試

作為其惡意軟體防護測試的後續行動，MRG Effitas 還發布了一份報告，比較不同端點解決方案阻止特定的入侵攻擊技術。Sophos Intercept X 遙遙領先其他受測的解決方案。事實上，與其他受測試的大多數工具相比，Sophos 能夠阻擋兩倍以上的入侵攻擊技術。



此處可取得完整報告。

Gartner 端點防護平台魔術象限

Gartner 的端點防護平台魔術象限是一項研究工具，評比廠商的願景完整性和執行能力。Sophos 連續十年被列入 Gartner 端點保護平台魔術象限的「領導者」。Sophos 是僅有的三家被列為領導者的廠商之一。

Forrester Wave™: 端點安全套件

Forrester Research, Inc. 進行了廣泛的產品評估，並訪談了多家端點廠商及其客戶後發布了一份報告。他們是根據產品強度及其策略來評估廠商。Sophos 再次名列 Forrester Wave 端點保護套件的領導者。

此處可取得完整報告。

ESG Labs Intercept X 產品評測

Enterprise Strategy Group Lab 測試了 Sophos Intercept X 之後確認：

「Intercept X 阻擋了 100% 的入侵攻擊手法，而它們正是傳統防毒應用程式無力防止的。」[3]

此處可取得完整報告。

擴充您的安全：選擇完全防護

端點安全解決方案只是整體安全策略的一環。現今的組織是明智的，他們要求不止保護端點，更要保護整個環境。

理想情況下，單一廠商提供的解決方案可以協同合作，為您的整個組織提供一致的保護和政策實施。與單一廠商合作可提供較好的安全性，減少系統管理負擔並降低成本。

有些特定技術要與端點保護必須一起考慮，包括全磁碟加密、行動裝置管理、行動安全、安全電子郵件閘道、專屬伺服器，或虛擬機器保護，以及端點與網路裝置之間的同步安全性。

評估端點安全：要詢問的十大問題

在評估端點保護解決方案時，請先詢問廠商下列問題：

1. 該產品使用基本技術、現代技術，還是結合兩者？該技術的核心是哪一個特定功能？
2. 該產品如何偵測未知威脅？它使用機器學習嗎？
3. 如果產品宣稱使用機器學習，請問使用的是哪一種機器學習類型？訓練資料來自哪裡？該機型投入生產多久？
4. 防範入侵攻擊型和無檔案型攻擊的技術是什麼？採用哪一種防入侵攻擊技術，以及可偵測哪些攻擊類型？
5. 該產品是否具備專為阻擋勒索軟體而設計的技術？
6. 廠商是否有佐證其方法有效的第三方結果？
7. 該產品的誤報等級是否在可接受範圍？如果偵測到誤報，減少影響有多容易？
8. 廠商提供哪些攻擊可見度，例如根本原因分析？
9. 該產品是否自動回應威脅？它是否會自動清除威脅及回應事件？
10. 部署及使用該解決方案會有何種程度的影響？

結論

隨著網路威脅的複雜度和數量不斷增加，端點上具備有效保護比以往更加重要。了解您必須阻擋的威脅，以及可用的不同安全技術，可讓您對端點安全做出明智選擇，並使貴組織獲得可防禦現今攻擊的最佳保護。

來源：

1 Sophos 端點安全狀態報告，2018 年 1 月

2 Sophos 端點安全狀態報告，2018 年 1 月

3 MRG Effitas 比較惡意軟體防護評估，2018 年 2 月

Gartner 端點防護平台魔術象限、Ian McShane、Eric Ouellet、Avivah Litan、Prateek Bhajanka，2018 年 1 月 24 日，Gartner 不對被列入研究報告中的廠商、產品或服務提供保證，也不建議技術使用者僅選擇最高評等的廠商。Gartner 研究報告中包含 Gartner 本身研究機構的觀點，但不應被當成事實的陳述。Gartner 不提供任何與這項研究有關的明確或暗示擔保，包含對適售性或特定用途適用性的擔保。

The Forrester Wave™: 端點安全套件，2016 第 4 季，作者 Chris Sherman，2016 年 10 月 19 日