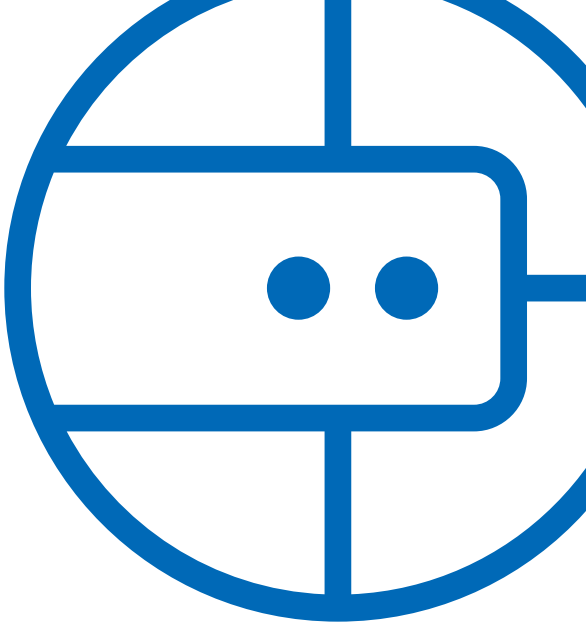
SOPHOS
Cybersecurity made simple.



伺服器保護方案購買指南

伺服器面對的網路威脅在複雜度和惡性方面持續以驚人的速度發展，如 WannaCry 和 NotPetya 等具破壞力的勒索軟體事件凸顯了對強大的反勒索軟體功能的需求。而Spectre 和 Meltdown 等利用系統性漏洞的攻擊表明，反漏洞利用和應用程式控制 (“預設拒絕”) 也是任何伺服器安全方案的關鍵環節。

由於伺服器通常是組織最有價值的端點，因此 IT 管理員面臨著必須選擇高效保護的壓力。在伺服器上執行桌面型安全解決方案是不夠的，您必須在伺服器核心部署包含伺服器工作負載保護的解決方案。

本指南為您提供在選擇伺服器安全所需的關鍵特色和功能的實用建議，以及要求廠商確保功能可完全正常運作的問題。

伺服器環境

根據組織的需要，您可能會在本地預置運作自己的伺服器、使用 Amazon Web Services (AWS) 或 Microsoft Azure 在雲端託管資料，或是混合使用兩者。因此，您需要一個可透過單一管理平台輕鬆管理這些不同部署的安全解決方案。

理想情況下，該解決方案可提供額外的優點，例如可以集中管理整個伺服器的一致性政策部署。自動部署雲端伺服器保護 (例如透過編寫指令碼) 非常重要，因此在必要時可以不經伺服器系統管理員的介入加以啟動 (和關閉)，以滿足需求。

隨著組織傾向選擇混合部署環境，簡單的授權許可證選項比以往任何時候都更加重要。請尋找可提供單一授權類型的廠商，無論是雲端、本地預置還是兩者混合，都可以避免複雜的搭配程序。

主要產品功能和特性

現代伺服器安全已經發展到可以領先先進威脅一步。為了確保伺服器安全，無論是在本地預置還是雲端，您都應該尋找這些可以抵禦未知威脅、勒索軟體，漏洞利用攻擊和駭客的功能：

- **反勒索軟體 (anti-ransomware)** - 一些解決方案包含專門用於防範勒索軟體惡意加密資料的技術。通常，這些技術 (特別是反勒索軟體) 也會修復任何受影響的檔案，例如將檔案回復到未受影響的狀態。勒索軟體解決方案不僅應該阻擋以檔為目標的勒索軟體，還應該防止破壞性抹除攻擊中用來篡改主開機記錄的磁碟勒索軟體。而且，伺服器還需要阻止遠端/惡意端點加密網路共用或其他已連線伺服器上的檔案。

- **伺服器鎖定/白名單/預設拒絕 (Server lockdown/whitelisting/default deny)** - 藉由將許可的應用程式列入白名單，防止未經授權的應用程式在伺服器上運作。購買者應該尋找能夠自動識別可信任應用程式的解決方案，同時還可允許使用者自行定義，以大幅減少建立安全規則集所需的時間和精力。此外，鎖定或解鎖伺服器時應該不用停機。

- **反漏洞利用 (Anti-exploit)** - 反漏洞利用技術是藉由阻止攻擊鏈中使用的工具和技術來阻擋攻擊者。例如，EternalBlue 與 DoublePulsar 等漏洞利用攻擊是用來執行 NotPetya 與 WannaCry 勒索軟體。反漏洞利用技術可阻擋用來散播惡意軟體與執行攻擊的相對較少的技術，而不需要事先看過它們 (不需要特徵碼)，因此能抵禦許多零時差攻擊。全方位的漏洞利用防護還可以為無法快速修補的伺服器提供保護，即使沒有可用的修補程式時也是如此。

- **反駭客 (Anti-hacker)** - 伺服器是駭客的主要目標，因為它們通常保存著組織最敏感的資料。請尋找包含專屬功能的解決方案，以阻止實時發生的駭客持續性攻擊。伺服器所需的反駭客緩解措施包含憑證擷取防禦、橫向移動防禦、程式碼洞穴緩解、權限提升保護和處理序移轉保護等。

- **機器學習 (Machine learning)</122** - 提供多種類型的機器學習方法，包括深度學習神經網路、隨機森林、貝氏定理和叢集。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出已知與未知的惡意軟體，而不需要特徵碼。機器學習的優點在於它可以偵測到從未見過的惡意軟體，在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。

[1] Gartner Top 10 Security Projects for 2018

- **事件回應/同步安全性 (Incident response/Synchronized Security)</124** - 伺服器工具應該至少能提供已發生的情況的深入資訊，以便避免將來發生的事件。在理想情況下，它們應該能自動回應事件而無需分析人員介入，以便阻止威脅擴散或造成更多損害。事件回應工具和其他伺服器安全工具、網路安全工具進行通訊非常重要。此外，您選擇的解決方案應該能夠向您展示攻擊是如何發生的，還有進入點、惡意處理序和受影響電腦的進一步詳細資訊 (例如根本原因分析功能)。

- **應用程式控制 (Application control)** - 控制哪些應用程式可以在伺服器上運作以減少受攻擊面。在理想情況下，廠商會按類別過濾應用程式以簡化和加速設定的工作。

- **集中管理 (Centralized management)</128** - 主控台應該能夠讓您輕鬆管理和監看混合的伺服器環境，例如警示、事件和報告，這些資訊都可以彙整到一個易於使用和瞭解的檢視中。

- **工作負載探索和保護 (Workload discovery and protection)</130** - 能夠探索在公用雲環境 (基礎架構即服務) 中運作的工作負載，例如 Amazon Web Services (AWS) 和 Microsoft Azure。眾所周知，攻擊者會利用未使用的雲端領域並將其用於其他方面，例如加密。可透過原生 API 與公用雲平台整合的產品可以標記新的工作負載執行個體，包括尚未主動使用的領域。

記錄與報告

除非出現問題，否則大多數情況下您都不會登入伺服器。就管理方面來說，有兩個主要要求：

1. 直接部署和監控所有伺服器
2. 介面易於使用，可讓您在出現問題時快速回應

許多時候，為不同環境中的個別伺服器部署來自多個廠商的單點解決方案，會因主控台過多而構成管理挑戰。在處理規模較大的伺服器資產時，這種情形很快就會成為一種負擔。因應嚴重的攻擊時需要快速、果決的行動，不能因為浪費時間找出決策所需的關鍵資訊而受到阻礙。請尋找可以將資訊整合到「單一介面」上的解決方案，盡可能使其能輕而易舉地找到重要的資訊。

某些解決方案還可以將您的伺服器與網路安全 (防火牆) 整合，並共享威脅情報。例如，如果伺服器被判斷為已遭駭，則可以將它與網路隔離，防止其對組織造成進一步損害。還可以準確地看到來自伺服器的流量和應用程式，以便根據重要應用程式的優先性排序或拒絕不需要的應用程式。

便於部署且允許透過腳本架設　(特別是對於雲端部署)，意味著伺服器系統管理員的時間可以用於其他用途。與純手動設定相比，預設拒絕應用程式白名單或以類別為基礎的應用程式控制可以更快速地設定允許和不允許在伺服器上運作的內容。

產品比較清單

在閱讀前述章節確定基本要求後，請使用此表來衡量不同廠商的解決方案，並評估它們對貴組織的適用程度。

產品特色比較			Intercept X Advanced for Server	Trend Micro Deep Security	Symantec Cloud Protection	McAfee Server Security Suite Advanced	Kaspersky Hybrid Cloud Security
管理		平台	雲端	雲端/預置部署	雲端	預置部署	預置部署
		單一主控台可以保護伺服器、端點、行動、電子郵件和無線網路	✓	×	×	×	×
		AWS/ Azure 工作負載探索	✓	✓	✓	✓	✓
		自動掃瞄排除項目 (例如 Exchange、SQL Server)	✓	×	✓	×	×
		虛擬化：使用集中掃瞄程式的精簡型代理程式	✓	✓	×	✓	✓
防禦	減少受攻擊面	Web篩選 (阻止惡意網站)	✓	✓	✓	✓	✓
		Web控制 (控制對可能不當站台的存取)	✓	×	×	×	✓
		應用程式白名單 (伺服器鎖定)	✓	✓	×	✓	✓
		以類別為基礎的應用控制	✓	×	×	×	×
		周邊設備/裝置控制	✓	×	×	×	✓
	在運作之前	機器學習 (深度學習)	✓	✓	✓	×	✓
		漏洞利用防禦	✓	✓	✓	✓	✓
		資料遺失防禦	✓	×	×	×	×
偵測		反駭客 (例如憑證竊盜和程式碼洞穴防護)	✓	×	×	×	✓
		勒索軟體保護 (行為偵測和回復)	✓	✓	×	×	✓
		磁碟和開機記錄保護	✓	×	×	×	×
		檔案完整性監控 (FIM)/變更監控	×	✓	✓	✓	✓
		惡意流量偵測	✓	✓	×	✓	✓
回應		同步安全(可與防火牆立即使用)	✓	×	×	×	×
		根本原因分析 (RCA)	✓	×	×	×	×

集中安全

保護伺服器是組織安全策略的重要一環。但是考慮到還有其他端點裝置、行動電話、網路安全和加密等保護措施，管理這一切可能有難度。實際上，對於許多廠商而言，每個新的安全領域都需要額外的主控台和政策框架，其中部分不甚相同，並且無法整合跨各種裝置和基礎架構元件的安全性。

Sophos Central 可讓您透過一個主控台管理所有的 Sophos 安全解決方案。它設計為單一平台，在不同產品之間操作時具有直觀且一致的介面。最重要的是，Sophos 的產品之間可以協同工作，為您提供更好的安全性。例如，伺服器與防火牆配合使用後，可在幾秒鐘內就自動識別、隔離和修復受感染的伺服器。

評估伺服器安全性：十個重要的問題

在評估伺服器保護解決方案時，請先向廠商詢問以下問題：

1. 該產品是否支援不同的伺服器部署，例如預置部署、雲端和混合部署？
2. 產品是否包含應用白名單/預設拒絕，而且無需額外費用？
3. 該產品是否具有專用於阻擋和回復勒索軟體的技術？
4. 防範漏洞利用和無檔案型攻擊的技術是什麼？採用哪一種反漏洞利用技術，以及可偵測哪些攻擊類型？
5. 該產品如何防禦主要威脅的持續性攻擊？
6. 該產品使用哪些技術來偵測未知的惡意軟體威脅？它是否使用機器學習？
7. 對於聲稱利用機器學習的產品，它們是否提供經第三方確認的偵測準確度？誤報率如何？
8. 廠商提供什麼樣的攻擊可見度，例如根本原因分析？
9. 產品是否能自動回應威脅？它是否會自動清除威脅及回應事件？
10. 產品是否可以與公用雲 (例如 AWS/Azure) 原生整合以自動探索雲端工作負載？

結論

隨著網路威脅在複雜性和惡性方面不斷發展，在伺服器上實施有效保護非常重要。了解威脅以及阻止它們所需的關鍵安全技術，讓您能夠為組織選擇最佳的伺服器保護方案。此外，您還需要考慮伺服器工作負載來設計保護措施。只是運作未能適應伺服器環境的端點保護是不夠的。