SOPHOS

# 網路安全系統購買者指南

83% 的 IT 管理員一致認為，在去年網路威脅變得越來越難以阻止，因此有越來越多的組織考慮放棄孤立的安全單點產品，改用彼此互連的網路安全系統。

選擇網路安全系統是一個大決定。隨著許多廠商談論跨產品整合，您應該尋找什麼什麼樣的系統？如何確保選擇正確？

在本指南中，我們將探討選擇網路安全系統時需考量的關鍵因素。我們也將了解 Sophos Synchronized Security 系統對比其他廠商 (包括 Fortinet、SonicWall、Cisco、Palo Alto Networks 和 Microsoft)。

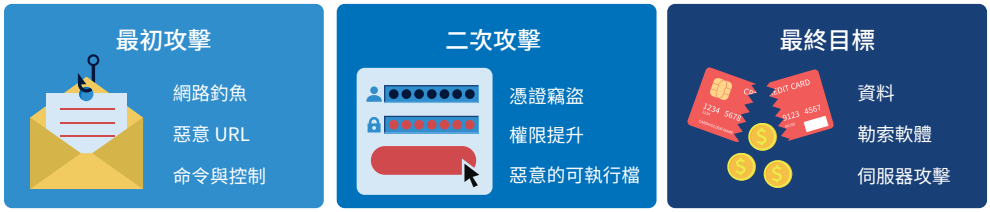
# 單點產品已經力有未逮

儘管技術不斷改進並投入大量資金，但現實情況是，網路安全對於現今的組織來說沒有變得越來越輕鬆。實際上，87% 的 IT 管理員認為惡意軟體威脅在過去一年中變得更加複雜，企業平均每個月要花七個工作天來識別和修復受感染的電腦。

### 網路安全以系統運作

若要了解這些問題的根本原因，我們必須先了解我們嘗試阻止的威脅。網路犯罪分子在其攻擊中不會使用單一手法和技術，而是在相互連線、協調的攻擊中使用多種手法。

例如，他們可能會從包含惡意 URL 的網路釣魚電子郵件開始。只要按一下該郵件，您就會被連線到命令和控制中心。他們可以結合使用憑證竊盜、權限提升和惡意可執行檔來實現最終目標，也就是竊取您的資料，或綁架您的資料以獲得贖金。




未連線的單點安全解決方案很難對抗這些複雜、協調的攻擊。這就是網路安全系統發揮長才的所在：讓多種整合式產品共同努力，打敗當今的駭客。

> **系統**，名詞。
>
> 形成一個統一整體的一組定期交互作用或相互依賴的項目。
>
> 來源：Merriam-Webster

### IT 基礎架構以系統運作

IT 系統是組織有效、安全營運的基礎。這種裝置、網路、資料和工作負載的連線網路可讓使用者以高效率進行 - 共用資料、存取、追蹤活動。

隨著技術的發展，我們的 IT 系統也在不斷地發展，行動裝置和雲端型工作負載與更傳統的要件並駕齊驅。雖然這種 IT 擴展是業務推動的主力，但它也為當今的組織帶來了可見度挑戰：只有 16% 的 CISO 能夠收集、分析和回應 75% 以上的安全事件遙測。

看不到就無法控制。網路安全系統可以透過關聯並整合來自整個 IT 基礎架構的資料，深入了解整個組織內的安全風險和使用者行為。它可讓 IT 看到隱藏的威脅，並採取明智的行動。

## 構成系統的要素

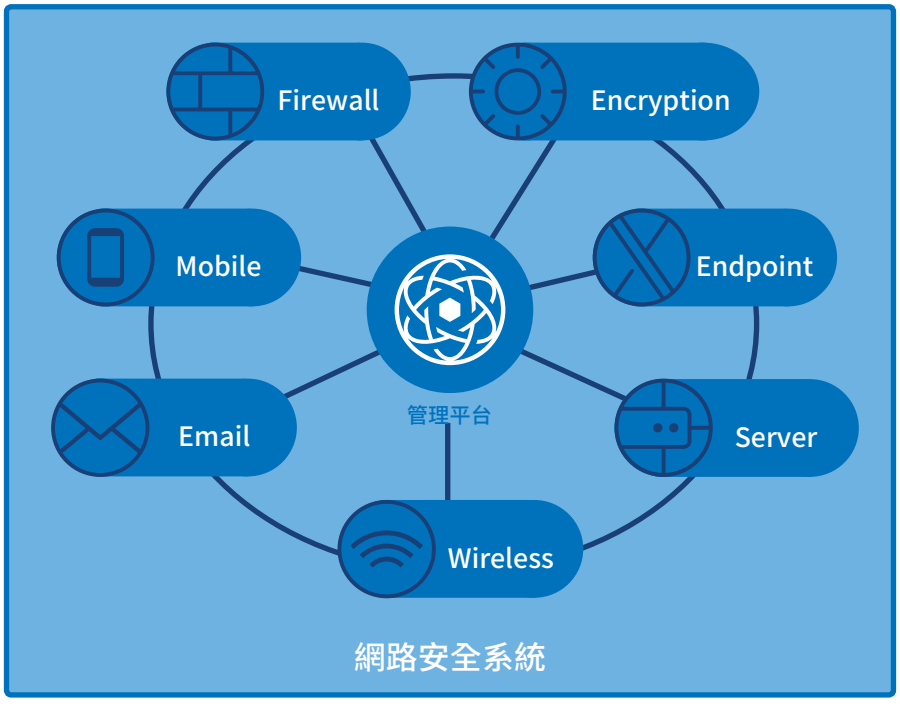
雖然越來越多的安全廠商在談論跨產品整合和網路安全系統，但他們的想法可能會有很大的差異。考慮到這一點，使用者值得花點時間考慮一下網路安全系統到底是什麼。任何有效系統的核心都有四個核心要素：

1. **中央管理：**在單一位置檢視並控制所有功能
2. **整合的元件：**不同的要素以和諧的方式共同運作
3. **自動化動作：**基於預先議定標準的循序行為
4. **可擴充性：**系統可以隨著需求的增長而成長

**中央管理、整合式元件、自動化動作和可擴展性都是網路安全系統的核心**

這四個要素是將單點產品轉型為系統的原因。這些元件越強，系統越強。深度整合的系統將優於具有未充分整合的系統。

同樣的原則適用於網路安全。網路安全技術平台是系統的核心，可讓 IT 團隊能夠透過單一介面，管理所有安全服務 (端點保護、防火牆、行動電話、電子郵件、無線網路、加密、使用者教育)。這些服務會主動地協同運作、共享資訊，並自動回應問題和事件。整合程度越大，系統的效率越好。



# 為企業提供價值

網路安全系統應該為整個企業和 IT 團隊增加價值。有效的解決方案將讓您：

- **降低網路風險：**減少暴露在攻擊之下，並在發生感染時大幅縮短回應時間。
- **提高可見度：**深入並廣泛地了解整個系統的安全性，讓您能夠做出明智、準確的決策。
- **提高生產力：**降低網路安全對 IT 團隊以及整個組織中的使用者的影響。
- **節省金錢：**您可以透過從單點產品移轉至網路安全系統來減少上線、整合和培訓成本，以及日常的系統管理開銷。採購和法務等非 IT 職能也可以從整合廠商中受益。
- **證明安全的價值：**網路安全系統可以透過減少修正日常問題所花費的時間，讓 IT 團隊能夠專心處理以業務為中心的專案。增強的防護功能以及因而減少的使用者停機時間也可讓更廣泛的組織能夠體會安全的價值。

# 如何選擇網路安全系統

若要從網路安全系統中獲得最大收益，必須考慮四個關鍵因素。

1. **保護範圍**

   也許您不需要或不想要立即採用全功能的網路安全系統，但應該確認日後可以選擇性進行擴充。多數人會從小系統開始(例如兩個安全元件共同運作)，然後在準備就緒時擴充，以納入其他解決方案。為了確保您的投資能夠因應未來需求，請確保您的系統能夠隨業務而增長。

   - **安全服務範圍：**網路安全系統有多廣泛？如果您需要，可以使用哪些產品？它能夠滿足您更廣泛的網路安全需求還是僅著重在一個領域？
   - **元件之間的通訊：**產品如何共享資訊？具有簡單單向通訊的產品，在系統中只能充當其中一部份，只能提供有限的效益。反之，在系統中持續共享資訊的產品可提供相當廣泛的安全性和資源優勢。
   - **輕鬆擴充：**將新產品加入到網路安全系統有多容易？使用新技術上線並運作又有多容易？
   - **其他成本：**您是否需要購買其他產品或訂閱才能獲得網路安全系統，超越個別解決方案的好處？在考慮成本時，請同時考慮購買安全產品的成本以及培訓和上線的成本。

2. **產品整合**
安全系統的重點不僅僅是超越各個部分的效用總和。各個產品共同運作可提供單獨產品無法實現的優勢。安全系統的核心優勢分為兩大陣營：自動化和可見度。需探索的主要領域包括：

   - **無須使用者介入、自動回應：**產品如何共同運作以便將以前的手動任務自動化？它提供哪種等級的自動事件回應？例如，如果偵測到感染，系統只是加上旗標，讓系統管理員採取行動，還是自動保護裝置、清除感染，然後在系統恢復良好狀況時重新連線？
   - **跨產品可見度：**產品整合如何提升整個組織的可見度？它是否可以提供即時事件分析與跨產品報告，為您提供可以採取動作的即時深入資訊？它在幫助您識別未知威脅方面實用嗎？

> 網路安全系統應該提供無須使用者介入的回應以及跨產品可見度。

在考慮產品整合時，請思考對您的組織最實用的是什麼。您需要考慮您的挑戰是什麼，以及哪些系統功能對您最有利。

3. **營運效率**
系統越容易使用，您就越能利用它所提供的功能。相當複雜且難以使用的解決方案效益有限，而且對於需要負責管理的 IT 團隊來說可能是麻煩的。需要著重的特定領域包括：

   - **可用性：**您可以多快且多輕鬆地部署、監控和管理系統？您需要使用多少管理主控台？您可以集中在單一位置做的事越多越好。
   - **費用：**系統是雲端架構還是需要資助並維護內部部署伺服器？
   - **一致性：**畫面和視覺表示在顯示上是否一致？一旦您熟悉了一種顯示方式之後，您是否可以輕鬆地解譯其他顯示方式，或者它們看起來有什麼不同？

4. **產品領導地位**
改用 Synchronized Security 系統後不應該在保護方面有所妥協。您應該充分利用端點和網路方面皆兩全其美的產品。從獨立使用時很優異，整合在一起時更棒的產品開始。

   - **業界驗證：**尋找在功效測試 (例如，SE Labs、AV-Test) 以及市場分析師評等 (例如 Gartner 魔力象限評論) 中表現良好的產品。
   - **客戶回饋意見：**使用網路安全系統的客戶會說什麼？他們享受了哪些好處？以及，它是否兌現了承諾？
   - **公認的領導者：**考慮使用產業分析師公認為領先的產品。

# 各家防火牆廠商防護比較

## 保護範圍

| 安全產品 | Sophos Synchronized Security | Fortinet Fortinet Security Fabric | Microsoft Intelligent Security Graph | SonicWall Capture Cloud | Cisco Stealthwatch 和 Identity Services Engine (ISE) | Palo Alto Application Framework |
|---|---|---|---|---|---|---|
| 端點 | ✓ | ✓ | ✓ | ✓ (SentinelOne) | ✓ | ✓ (Traps) |
| 端點偵測與回應 (EDR) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 伺服器 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 防火牆 | ✓ | ✓ | | ✓ | ✓ | ✓ |
| 郵件 | ✓ | ✓ | | ✓ | ✓ | |
| 行動設備 | ✓ | | ✓ | | ✓ | |
| 無線 | ✓ | ✓ | | ✓ | ✓ | |
| 磁碟加密 | ✓ | | ✓ | | | |
| 安全警覺性培訓 | ✓ | | | | | |
| 雲端型工作負載 | ✓ | ✓ | ✓ | | ✓ | ✓ |
| 產品共同運作所需的其他訂閱 | | ✓[1] | | | ✓[2] | ✓[3] |

1.在 Security Fabric 中整合 FortiClient 所需的 FortiGate Endpoint Telemetry and Compliance 授權。在 FortiAnalyzer上的IOC 服務去了解受駭主機的資訊。

2.需要 Cisco Network Orchestrator Trusted Access。

3.需要威脅防禦/WildFire 訂閱。

# 產品整合

| | 無須使用者介入的自動回應 | 跨系統可見度 |
|---|---|---|
| **Sophos**<br>Synchronized Security | ‣ 透過 Security Heartbeat™ 持續監控裝置健康狀態，實現自動事件回應<br>‣ 偵測到任何地方受到感染時，自動隔離受駭的端點：端點或網路<br>‣ 橫向移動防禦可以阻止穿越網路的威脅<br>‣ 自動限制受駭端點的 Wi-Fi 存取<br>‣ 自動限制非合規行動裝置的 Wi-Fi 存取<br>‣ 偵測到惡意電子郵件時，自動掃描端點裝置<br>‣ 偵測到惡意軟體或入侵者時，自動撤銷加密金鑰 | ‣ 同步應用程式控制會識別網路上的所有應用程式，包括先前未知的網路和雲端應用程式<br>‣ 威脅案例會提供事件的完整事件鏈，包括相關的所有檔案，以及與之通訊的 URL/IP<br>‣ 將網路流量與個別電腦上的個別應用程式相關聯 |
| **Fortinet**<br>Fortinet Security Fabric | ‣ 防火牆偵測到感染時，自動隔離受駭端點 | ‣ 顯示所有連線 Security Fabric 裝置的圖形<br>‣ 端點狀態監控可識別是否已安裝 FortiClient<br>‣ Security Rating 可顯示組織的安全態勢 (另外授權) |
| **Microsoft** Intelligent Security Graph | ‣ 端點調查可以在 Defender ATP 中自動觸發 | ‣ CASB 使用 Windows Defender ATP 用戶端識別未知的雲端應用程式<br>‣ Windows Defender ATP 和 Office 365 ATP 會共用資料以便透過端點執行，協助追蹤電子郵件傳遞的威脅 |
| **SonicWall**<br>Capture Cloud | ‣ 複雜防火牆部署與管理工作自動化<br>‣ 端點保護用戶端可簡化 TLS/SSL 認證的部署與管理 | ‣ Cloud App Security (CAS) 提供雲端應用程式的可見度 (需要 Analytics 授權) |
| **Cisco**<br>Stealthwatch 和 Identity Services Engine (ISE) | ‣ ISE 根據合規性和其他要素提供的網路存取控制<br>‣ Cisco Threat Response 可讓安全營運團隊手動調查並回應威脅 | ‣ Cisco AMP 會跨電子郵件、防火牆和端點，追蹤威脅 |
| **Palo Alto**<br>Application Framework | ‣ 回應能力取決於所使用的應用程式。系統通常會在網路層強制執行修復，例如阻擋 URL 或 IP 位址 | ‣ 應用程式可以從網路和端點存取安全情報 |

## 營運效率

| 管理效率 | Sophos Synchronized Security | Fortinet Fortinet Security Fabric | Microsoft Intelligent Security Graph | SonicWall Capture Cloud | Cisco Stealthwatch 和 Identity Services Engine (ISE) | Palo Alto Application Framework |
|---|---|---|---|---|---|---|
| 雲端託管管理 | ✓ | | ✓ | ✓ | ✓ | |
| 單一管理主控台 | ✓ | ✓ | | ✓ | | |
| 所有產品的通用介面 | ✓ | ✓ | | ✓ | | |

## 產品領導地位

| 產品領導地位 | Sophos 同步安全 | Fortinet Fortinet Security Fabric | Microsoft Intelligent Security Graph | SonicWall Capture Cloud | Cisco Stealthwatch 和 Identity Services Engine (ISE) | Palo Alto Application Framework |
|---|---|---|---|---|---|---|
| Gartner 端點保護平台魔力象限 (2018) | 領導者 | 特定領域者 | 遠見者 | 遠見者 | 遠見者 | 特定領域者 |
| Gartner UTM/企業防火牆魔力象限 (2018) | 領導者 | 領導者 | NA | 挑戰者 | 領導者 | 領導者 |

# Sophos 的同步安全 (Synchronized Security)

Synchronized Security 於 2015 年首次推出，將 Sophos 市場領先的端點和網路保護整合到一個功能強大、深度整合的網路安全系統中。Synchronized Security 的核心是 Sophos Central，這是一個直覺式的安全平台，可讓 IT 團隊能夠透過單一網頁型介面查看、管理和控制所有一切。產品可透過 Security Heartbeat™ 分享即時資訊，讓它們自動回應威脅，並提供前所未有的跨產品網路風險可見度。

客戶一致認為 Synchronized Security 將網路安全轉型。

**90%** 的客戶同意，使用 Synchronized Security 讓他們對網路流量擁有更大的控制權

**85%** 的客戶同意，Synchronized Security 改善了他們的安全狀態

**84%** 的客戶同意，Synchronized Security 能協助處理日益增加的 IT 壓力