除了應用程式可視性和控制外：NGFW 的必備條件

除了應用程式可視性和控制外：NGFW 的必備條件

您將會學到

新式網路和其元件正不斷進化，而傳統的新世代防火牆無法提供組織所需的保護等級。

在本文中您將瞭解到：

- 為什麼典型的新世代防火牆主要著重於應用程式可視性和控制，所提供的威脅防禦做法之所以不完整的原因
- 組織在資源受限的環境中需要什麼來擊退進階威脅
- 您可從業界第一個完全整合且聚焦於威脅的新世代防火牆 (NGFW) 思科 Firepower™ NGFW 獲得哪些效益

簡介

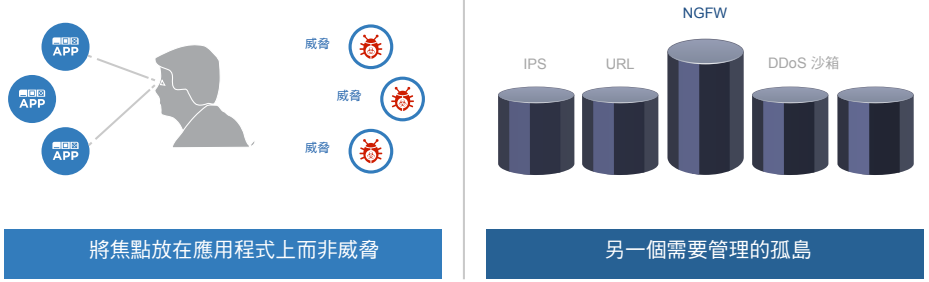
數位轉型正大規模進行中，而且創造了大量商機。目前有超過 150 億部裝置與網際網路連線，且預期這個數字會在 2030 年以前成長至 5000 億。[1] 這個轉型預期會在未來 10 年為全球帶來預估 19 兆美元的商機。[2] 然而，卻也為網路罪犯創造了大量機會。根據估計，全球網路犯罪市場目前為 4500 億至 1 兆美元。[3]

隨著新式網路和其元件不斷進化，攻擊面也跟著擴張。受金錢利益驅使的攻擊者正採用越來越複雜的方式來滲透網路，以及竊取數量不斷增加的數位化資產，一旦他們成功滲透網路，便很難偵測到他們。事實上，業界偵測進階威脅所需的平均時間約為 100 天。[4]

今日的網路安全挑戰

若要抓住數位經濟和新商業模式所創造的新興商機，資安是基礎所在。新世代防火牆 (NGFW) 的推出是一大邁進，不過典型 NGFW 將焦點放在應用程式存取控制，對於威脅防禦功能少有著墨。但是若要防禦老練攻擊者和進階惡意軟體所帶來的風險，這種不完整的做法幫助並不大。更糟糕的是，一旦組織遭感染，這些 NGFW 提供的援助有限，無法協助您調查、阻止和快速修復感染。

舊式 NGFW 的聚焦範圍太過狹隘而且難以管理



組織沒有資源可加入更多產品，也沒有資安人員可管理這套分段做法所帶來的額外複雜性。實際上，資源限制是欲採用更佳安全性時最常遇到的障礙。[5] 此外，以這些中斷連線的安全服務為基礎的架構相當脆弱，進而因作業缺乏彈性而抑制了企業成長。

1. 思科物聯網：http://www.cisco.com/web/solutions/trends/iot/indepth.html
2. http://ioeassessment.cisco.com/learn
3. RSA/CNBC：http://www.cisco.com/web/offer/emear/38586/images/Presentations/P16.pdf
4. 思科 2016 年度資安報告
5. 思科 2016 年度資安報告

NGFW 的必備條件

組織需要 NGFW 平台提供更多功能。他們需要可提供以下功能的新世代防火牆：

- 將焦點放在威脅有效性，並針對整個攻擊過程（攻擊之前、期間與之後）提供保護。
- 將所有資安服務與事件資訊完全整合至單一檢視畫面和管理平台中
- 整合現有資安投資，提供化零為整的更佳效果

符合這些要求的新世代防火牆不僅可藉由精準的應用程式控制帶來價值，也可提供真實世界的安全有效性，抵禦複雜且捉摸不定的惡意軟體攻擊所帶來的威脅，還可讓組織簡化作業並使其網路發揮更大效益。

思科 Firepower NGFW 簡介

思科 Firepower 新世代防火牆 (NGFW) 是業界第一個完全整合且聚焦於威脅的 NGFW，超越了傳統 NGFW，可在整個攻擊過程中提供完整的整合式保護。

採用思科 Firepower NGFW，便可立即擁有遠超過應用程式控制的整合資安平台，其強大的多重向量資訊關聯性有利於偵測規避或可疑活動，以及早期識別出現入侵跡象的主機。您可阻止更多威脅、獲得更優異的網路可視性、更快速偵測和減輕零時差與針對性威脅、自動化重要工作以便更專注於組織工作，以及利用現有資源獲得更大效益。

提供完整保護

思科 Firepower NGFW 中包含全世界部署最廣泛的可設定狀態防火牆技術，並搭配新世代 IPS、進階惡意軟體防護、應用程式可視性和控制，以及基於信譽的 URL 篩選功能。上述所有功能均囊括在單一設備中，且皆可經由一個功能多元的整合管理主控台進行管理。

阻止更多威脅

部署業界最有效的威脅防護，抵禦已知和浮現中的威脅。我們的 NGFW 具備一套整合沙箱解決方案以及檔案流行度與處置方式，可協助識別並阻止捉摸不定的針對性威脅，避免造成進一步損害。

獲得更多深入分析

獲得可視性，觀察不斷變動的網路中存在的使用者、主機、應用程式、行動裝置、虛擬環境、威脅和弱點，此資訊將能協助您防衛網路。NGFW 會自動建立威脅和網路弱點的關聯，讓您的資安團隊能判斷威脅的優先順序，把注意力集中在最重要的威脅上。

及早偵測，盡快行動

更快速減輕進階威脅，將偵測和修復用時從數月縮短至數小時。思科可在 17.5 個小時內完成工作。[6] 立即瞭解惡意軟體的感染範圍、路徑和檔案活動行為，甚至在簽章可用前採取遏止動作。

降低複雜度和簡化作業

將所有資安功能合併至一個具有單一管理介面的高效能平台上。思科 Firepower 管理中心可整合、集中和簡化政策，進而減輕管理深度防禦安全架構的負擔；還可自動分析網路弱點和建議防護措施，為現今不斷變動且人力不足的環境提供回應式解決方案。

讓您的網路發揮更大效益

思科 Firepower NGFW 與其他思科®資安解決方案整合，例如適用於身分資料及網路分段的思科身分識別服務引擎 (ISE)，以及適用於取得網際網路網域可視性的 OpenDNS。情報、內容和政策控制項皆可共用，讓這套做法有效、靈活且更易於管理，管理所需的費用也更為低廉。自動網路分段可協助您迅速遏止威脅。思科 Talos 的全球 DNS 和 IP 威脅情報提供極具聲譽的威脅指標，可用於早期警告，讓網路安全裝置可在攻擊抵達前準備防禦措施。

思科 Firepower NGFW 可讓客戶處於更安全的環境、更快速減輕進階威脅以及更有效簡化作業。安全性儼然成為成長引擎，可協助您掌握新商機。

深入瞭解

如需深入瞭解思科 Firepower 新世代防火牆，請造訪：www.cisco.com/go/ngfw

6. 思科 2016 年度資安報告

C11-736644-00 02/16