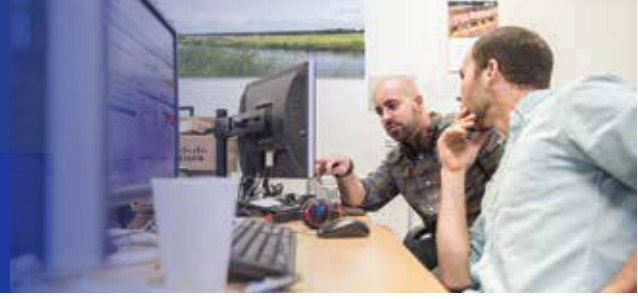
5 選擇的秘訣：新世代防火牆



投資一個專門阻擋威脅的新世代防火牆 (NGFW)。瞭解它是否提供

1 整合威脅防禦

取得可執行、多層級的保護。

現今的多向量和持續威脅不僅能從保護機制的空隙中潛入，也能成功躲避偵測。這款專門阻擋威脅的新世代防火牆 (NGFW) 提供業界最優秀的安全科技，能夠跨網路和端點配合運作，並透過中央主控台管理。建立在全方位狀態防火牆的基礎上，專門阻擋威脅的新世代防火牆 (NGFW) 科技特點包括：

- 新世代 IPS
- 進階惡意軟體保護
- 應用程式能見度和控制，
- 基於信譽的 URL 篩選應用程式
- 層級 VPN

▸ **藉由持續連結不同安全層級威脅情報的整合威脅及進階惡意軟體保護，您可以辨識和防禦精密複雜的攻擊。**

資源

新世代防火牆：投資檢查清單
白皮書：取得完整的檢查清單來保護您的企業免受攻擊。立即閱讀。

TechWise TV：思科 Firepower NGFW
查看以防禦威脅為優先的完全整合安全性解決方案。觀看影片。

思科 NGFW 網站
掌握最新趨勢並瞭解思科提供了哪些關於安全性的新功能。
瞭解詳情。

2 可執行的入侵指標

加速惡意軟體偵測以降低風險。

現今業界偵測單一威脅所需的標準時間為期 100 天至 200 天，這實在是太長了。新世代防火牆 (NGFW) 應提供可執行的入侵指標 (IoC)，其功能有：

- 聯結網路和端點安全情報
- 提供針對可疑和惡意檔案的高精確能見度，
- 以及主機行為應優先遭感染的主機以快速修復

▸ **可執行的 IoCs 讓您檢視惡意軟體在主機和端點的活動，理解其影響並快速加以遏阻和修復。**

3 全方位網路能見度

透過全方位檢視提升安全效能。

Y您無法保護看不見的地方。您需要隨時監控您的網路狀況。新世代防火牆 (NGFW) 提供完整的環境感知：

- 使用者、作業系統以及虛擬機器
- 威脅和漏洞之間的
- 裝置通訊
- 應用程式和網站存取檔案
- 傳輸，以及其他

▸ **此層級的深入洞察能幫助您辨識並處理安全性間隙和調整政策，由此減少需要其他動作的重大事件數量。**

4 降低複雜性和成本

統一安全層級並自動化以增加效率。

進階威脅和 IT 安全性專業人才短缺這兩大問題讓 IT 部門倍感壓力，希望尋找具備以下功能的新世代防火牆 (NGFW)：

- 合併多層級防禦至單一平台，
- 提供一致且健全的大規模安全性
- 自動化固定程序安全性作業，例如影響評估、原則調整和使用者辨識

▸ **透過降低複雜性和成本，您的團隊無須擔心瑣事，能夠專心在最重要的工作上。**

5 整合第三方解決方案

讓現有的安全性投資發揮最大效用。

您需要能夠分享情報，以及更有效地發揮現有的安全性科技以合併並精簡回應。尋找一個開放的新世代防火牆 (NGFW)，其能夠與第三方安全性解決方案的生態系統順利整合，例如：

- 漏洞管理系統
- 網路視覺化和 SIEM 系統
- 工作流程修復和售票系統
- 網路存取控制 (NAC)，以及其他

▸ **整合第三方解決方案減少您的 IT 人員負擔和整體擁有成本 (TCO)，並加強多層級保護。**

攻擊將會持續演化，您需要防護的 IT 環境也必須持續改進。確保您所選的新世代防火牆 (NGFW) 具備**緊密整合、多層級的威脅防護。**藉由分享背景資訊和情報來加速您組織內的威脅偵測和回應，讓您的投資發揮最大效用。

CISCO

關鍵不在我們已經達成什麼；而是我們帶來多少新的可能。

實現全面的安全性。

請造訪 www.cisco.com/go/ngfw

追蹤我們的 Twitter 帳號 Twitter @CiscoSecurity