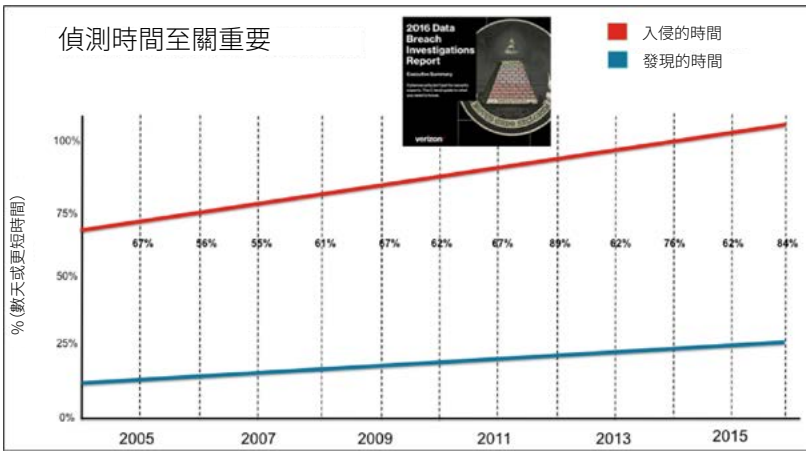
Fortinet Security Fabric 與威脅概況

簡介

網路的進化極具諷刺意義，我們開發的應用程式、資料和服務以更快的速度流入日益多元化的使用者、裝置和網域環境，是我們自己加劇了保護這個新環境的複雜性。

那是因為，我們仍不斷向已是不堪重負的安全庫增加新的安全裝置，令其雪上加霜。但不斷增加的網路入侵事件提醒著我們，上述方法並非解決問題的良策。事實上，雖然您所購買和部署的新裝置可能會縮短發現新威脅所需的時間，但數據顯示，與過往相比，攻擊侵害您網路所需的時間已大大減少，而您尚未作好準備。



我們所面臨的挑戰中，複雜性正是安全大敵。孤立的安全性解決方案採用單獨的管理介面，並無蒐集或與網路上其他裝置共用威脅資訊的有效方式，作用十分有限。我們需要的是一個遍及網路、協同式的安全工具生態系統。該系統涵蓋物聯網到雲端，經過精心設計，可協同作業，提供無縫隙的安全防護。它能夠監測裝置和網路流量，智能分隔網路，共用和關聯本地和全球威脅情報，並協同工作以消除攻擊鏈上的任何威脅。

Fortinet Security Fabric

我們需要一種全新的安全防護方式。Fortinet Security Fabric（安全織網）是一種架構式的方法，首次將分散的安全性解決方案整合為一個整體。這種織網式方法具有五大關鍵屬性：

1. **擴展性** - Security Fabric 將安全性與網路技術相整合，因而安全性原則和執行可擴展到您的整個分佈式網路，以更有效地保護不斷變化的網路環境和應對新生的威脅挑戰。

2. **警覺性** - Security Fabric 將端點、存取層、網路、應用程式、資料中心、內容及雲端的安全性整合為一個單一的協作解決方案，以便能夠共用威脅情報、識別多數孤立的安全性解決方案難以發現的複雜威脅，並自動協調有效回應。

3. **安全性** - Fortinet Security Fabric 採用了前所未用的分層式防護來保護您的分佈式資產。Security Fabric 將新一代的偵測和回應系統、智慧型網路分段和單一虛擬管理介面相結合，能夠持續觀察並對目前最複雜的威脅作出回應，同時進行動態調適，以適應不斷變化的網路架構。

4. **可執行性** - 透過統一的分析和管理介面，實現即時的全球與本地威脅情報共用，對於網路罪犯所採取的新威脅策略和發動的零日攻擊，Security Fabric 均能採取動態回應予以反擊。

5. **開放性** - Security Fabric 採用一系列開放的 API（應用程式開發介面）、開放的身份驗證技術和標準化的遙測資料進行設計，不同組織均可將其聯盟夥伴所提供的現有安全性投資整合到 Fortinet Security Fabric 中。這些解決方案可以主動蒐集和共用威脅資訊並發佈安全緩解說明以完善威脅情報，提高威脅警覺性並擴大端到端之間的威脅回應。

應對威脅的生命週期

攻擊通常有四步程序。威脅生命週期的四步程序包括準備、滲透、駐留和傳播。視攻擊能力而定，網路罪犯可以對網路進行全面評估，利用發現的弱點進入網路，置入 rootkit 或類似軟體以避免被發現，然後全面深入網路以尋找資料或資源加以利用或進行竊取。該程序的每個步驟分別使用特定的工具和技術、共用獲得的資訊，通常由攻擊者集中管理指揮。

為了作出有效的回應，您的安全性部署能力需要在被攻擊者利用的資源方面有所體現。Fortinet Security Fabric 將下述重要的安全性功能與面向威脅的架構相整合，此類架構專門用於監看和阻止攻擊，即便是瞄準企業中最偏遠角落的最複雜的攻擊，也無處藏身。

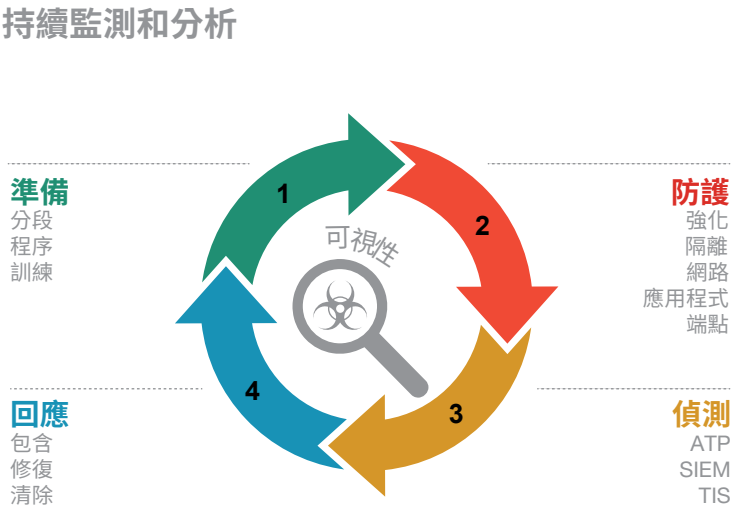
可視性 - 對於看不到的攻擊，防護便無從談起。透過 Fortinet Security Fabric，您可以識別網路中的各種元素，查看這些組成部份如何相互協作，識別潛在的攻擊手法，建立和實施更有效的原則和防護策略。

網路分段 - Security Fabric 可以智能地將您的網路分隔為數個功能安全區。透過從物聯網到雲端並跨越實體和虛擬環境的端到端分段，您可以深入觀察橫向穿越分佈式網路的流量、限制惡意軟體的傳播，同時還可以識別和隔離被感染的裝置。

自動作業 - Security Fabric 可在安全性裝置之間動態共用本地和全球的威脅情報，並能夠使用此類情報，在裝置之間集中協調協作式的威脅回應，阻止攻擊鏈上的任何威脅。

安全性稽核 - Security Fabric 的集中管理和新一代 SIEM 技術可以確定和監測不同的網路分段之間的信任層級，蒐集即時威脅資訊、確立統一的安全性原則、基於安全性狀況作出建議，並在廣泛的網路中部署適當的原則。

這一功能被引入 Fortinet 的四步威脅生命週期策略中，該策略主要用於應對網路罪犯所採用的攻擊策略。這四個步驟為：**準備**、**防護**、**偵測**和**回應**。



準備

若你知道有多少組織還沒有制定完整的安全性策略，定會感到大吃一驚。有很多組織甚至還沒有書面的安全性政策。他們通常只是根據需要向其網路中增加安全性裝置，而且幾乎都是在事件發生之後才這麼做。這就形成了典型的「隨意架構」難題，他們的安全性架構主要由一次性購買的孤立的安全性技術組成，用於解決不同的問題，並且基本不能提供全面的可視性。

準備一個安全的動態網路需要從以下三個基本元素開始：

1.端到端的分段

網路分段不僅在邏輯上分隔資料和資源，它還可以在資料和威脅從一個網路區域移動到另一個區域時，進行進階監測。從威脅的角度來看，網路分段將您的網路劃分為數個安全區，可協助遵從法規、監測內部流量和裝置、防止對受限制的資料和資源進行未經授權的存取，以及控制入侵者和惡意軟體的傳播。

Fortinet Internal Segmentation Firewall（內網隔離防火牆，ISFW）屬於 Security Fabric 架構的一部分，一旦威脅越過網路的外層防護後，它可透過智能分隔和在網路的邊界內側進行防護，阻止威脅擴散。ISFW 也可以用於防護包含寶貴的智慧財產權的特定伺服器，或安裝在雲端中，保護一系列的使用者裝置或網路應用程式。

2.程序

當網路已被分隔成獨立的安全區域後，下一步就是瞭解您的網路程序和程式。在準備程序中，您需要問幾個基本的問題：

- **使用者識別** - 誰在網路中？他們可以做什麼？他們何時進入網路？進行存取需要什麼憑證？
- **裝置識別** - 網路中有什麼裝置？它們的所有者是誰？它們可以做什麼？如果它們出現不良行為，我如何能發現？
- **實體拓撲** - 這些裝置如何與網路相連？允許與它們交互的其他裝置有哪些？不允許的有哪些？
- **網路和應用程式拓撲** - 我們需要什麼原則？它們是如何分佈和執行的？我們對整個網路是否有單一的管理介面？在某個原則被違反時，我們如何得知？在某個裝置上偵測到的違規能否觸發其他裝置上的自動回應？

接下來的重要步驟就是選擇專門解決此類程序性隱憂的安全解決方案。理想情況下，它們應該作為一個系統來協同工作，以對應、監測和防護您的分佈式網路，涵蓋範圍包括物聯網到雲

端。對整個分佈式企業的全局監看，以及在不同安全性裝置之間進行細密管控和協調回應的需求，正是 Fortinet 開發 Security Fabric 的主要動力所在。該軟體將資料、應用程式、裝置和工作流程緊密連結在一起，提供的警覺度和回應速度是其他安全程式提供商所不能及的。

Fortinet Security Fabric 包括：

- 端點用戶端安全性
- 安全（有線、無線和 VPN）存取
- 網路安全性
- 資料中心安全性（實體和虛擬）
- 應用程式（OTS 和自訂）安全性
- 雲端安全性
- 內容（電子郵件和 web）安全性
- 基礎結構（交換和路由）安全性

為了進一步提升組織的監看、管控和回應能力，Fortinet Security Fabric 的各組成部份不但可作為一整個安全系統工作，而且我們還開發了一系列的 API，允許 Fortinet 的聯盟夥伴透過 Fortinet Security Fabric 蒐集和共用資訊。

Security Fabric API 整合點包括：

- 雲端
- 虛擬化
- SDN 協調流程
- 端點和物聯網
- 弱點管理
- SIEM
- 管理
- 網路和安全性作業

然而，整合不僅僅是讓第三方解決方案蒐集或重新導向資料與流量。準備好與織網相連的聯盟解決方案可以與 Fortinet Security Fabric 主動整合，能夠對威脅資訊和緩解說明進行主動蒐集、共用和回應，進而完善威脅情報、提高整體的威脅警覺性，同時擴大了端到端的威脅回應。

3.訓練

當然，任何安全作業都需要納入訓練。訓練因情況而異，可能包括技術認證到簡單的員工警覺性宣傳，因為絕大部份的網路入侵事件仍是由於員工點擊意外收到的郵件或附件而造成。

此外，至關重要的是確保您的 IT 和安全團隊接受供應商的訓練，使他們能夠最大程度利用安全性技術投資的功能和特性。此項訓練還需包括如何利用開放的 API，允許不同的裝置更好地共用威脅情報和對威脅作出回應。

防護

多數組織將大部分的安全性投資花在了邊界的安全性上，試圖阻止不良企圖者和惡意軟體破壞其網路防護。但一些專家預測，到 2021 年，全球每年的網路犯罪成本將增長至高達 6 萬億美元，組織可能需要重新考慮要如何花費這些安全性投資。

由於網路日趨高度分散，使這一挑戰變得更加複雜，這表示，以邊界為基礎的安全性策略也越來越難定義和部署。為了幫助組織防禦當今複雜的網路威脅，有效的防禦策略需要包括如下方面：

- **存取控制** - 這就需要在傳統的網路存取層和資料、應用程式或工作負載每次嘗試跨越網路區域時實施控制。
- **強化邊緣裝置** - 除了防火牆和 VPN，組織還需要以安全性為前提，考慮部署路由器、交換機和無線存取點。任何沒有參與到安全性健全狀況和網路情報的裝置均存在風險。
- **隔離和修復** - 被入侵的裝置需要得到快速識別並從網路中移除以進行修復。
- **網路分段** - 由於在組織內，存取已變得越來越普遍，因此在新裝置（如物聯網）加入網路中時，很有必要將網路動態分隔為數個安全區域，以防止惡意軟體的傳播或限制對傳統網路邊界內的資料和資源的自由存取。
- **保護應用程式** - 應用程式的流量、工作負載，以及結構化和非結構化的資料都需要進行檢查和監測。為了能有效地實現目標，這一流程需要強大的處理能力，許多安全性解決方案都在努力做到這一點。
- **保護端點裝置** - 端點裝置對許多組織而言，仍然是一個實際存在的挑戰，尤其是 BYOD（自攜設備）和物聯網等裝置。它們通常是惡意軟體進攻的渠道，需要得到適當的強化，強化方式可以是透過安裝用戶端、藉由基於雲端的服務進行檢查或實施嚴格的存取控制和檢查。從安全的角度來看，應盡可能地將它們當作分佈式網路的延伸來對待。
- **將安全性擴展到雲端** - 流量、資源和應用程式已進入雲端，安全性也不能就此止步。在傳統、虛擬和雲端網路之間實施統一的監看、原則執行和威脅協調至關重要。

Fortinet Security Fabric 將端點、存取層、網路、應用程式、資料中心、內容和雲端整合為一個協同式的安全性解決方案，可透過單一的管理介面進行協調管理。

偵測

隨著組織不斷採用最新的數位化業務技術（如物聯網）、行動性技術、雲端服務和基礎結構，傳統的網路邊界正變得越來越難以控制和保障安全。

組織不能認為，在周邊布設防禦便已足夠。現在，進入企業網路的方法花樣繁多，網路侵害的問題不是是否會發生，二是何時會發生。最為常見的是，一旦駭客獲得對網路的存取權，他們就可有自由存取整個企業網路，包括其所有寶貴的資產。此外，網路罪犯可以長時間駐留在網路內，探索和發掘資訊，植入惡意軟體和竊取資料，給受害企業帶來災難性的後果。

Fortinet Security Fabric 包含三個重要的安全性元件，可以幫助偵測最為複雜的威脅：

進階威脅防護 (ATP) - Fortinet ATP 解決方案經過設計，可以防護、偵測和阻止當今最進階的威脅。它包含 FortiGate 防火牆、FortiMail 安全電子郵件閘道、FortiWeb web 應用程式防火牆、FortiClient 端點防護和使用 FortiSandbox 技術的主動式進階威脅偵測。領先的 FortiGuard Labs 安全性情報由 FortiSandbox 的本地情報補充，在互聯的安全性結構中動態共用。透過這一功能，ATP 部署便可自動回應最新的有針對性的攻擊，持續改善組織的安全性狀況，縮小多供應商產品之間的自然差距，同時減少 IT 安全性的管理時間。

FortiSIEM - 安全性破壞的事件平均需要將近八個月才能發現，而且通常僅是由第三方發現的。部分原因是，許多企業的安全性團隊需要在十幾個不同的安全性監控和管理控制台上進行追蹤，他們仍需要手動關聯事件和資料，來偵測當今能夠隱身的進階威脅。

FortiSIEM 是集多功能於一身的平台，能幫助全面深入洞察網路中發生的事件，讓您快速發現和修復安全性威脅和管理法規遵循標準，同時還能降低複雜性，提高關鍵應用程式的可用性和改進 IT 管理效率。

威脅情報服務 - Fortinet Security Fabric 採用 FortiGuard Labs 開發的安全性服務，功能強大，FortiGuard Labs 由遍佈全球的超過 200 名專業研究人員和分析師組成。這些研究人員採用公司內部開發的一流工具和技術，並結合使用從全球 200 萬台感測器蒐集到的資料，努力研究、偵測不斷變化的新威脅並加以抵禦。

基於對威脅環境的廣泛認知，加上與本地威脅情報相關聯，Fortinet Security Fabric 便可快速識別新出現的威脅並作出回應，隨後還可自動協調有效的對策。

回應

發現威脅只是打了一半的戰役。在識別威脅後，您需要能夠回答以下五個重要的問題：

1.威脅是如何來到這裡的？

2.它來到這裡花了多長時間？

3.有多少裝置被入侵了？

4.我如何將其從每一個裝置中移除？

5.我如何確保它不會再來？

FortiSandbox - FortiSandbox 是 Fortinet 進階威脅防護解決方案的組成部份，專門用於識別來路不明的進階威脅。識別到新威脅後，FortiSandbox 在偵測和防護產品之間自動利用直接情報共享，提供即時防護功能。它也可以提供輔助防護功能，讓人與技術共同合作，解決複雜的威脅挑戰，包括清理和修復。

Fortinet Security Fabric 的多個元件配合工作時，它們可以透過自動化和修復功能，對識別到的威脅採取強有力的回應。

自動化 - 只是識別威脅並發出警報尚不足夠。發生入侵的時間是很短暫的，有效的惡意軟體可以在幾分鐘內開始竊取關鍵資料。Fortinet Security Fabric 設計用於在偵測到威脅時，自動阻斷感染鏈，動態保護網路資源。

修復 - 修復策略包括隔離受感染的裝置、篩選出惡意軟體、阻斷對命令和控制的存取，以及鎖定關鍵的網路資源。這些經過協調的回應旨在用於識別和隔離受感染的裝置，以便可以對它們進行清理，然後再連接回網路中。從偵測到的威脅事件吸取了更多的防護方法和原則，這些防護方法和原則將應用到所有網段中，改善組織的安全性狀況和確保未來免受攻擊。

分層的方法

Fortinet Security Fabric 建立在一系列分層的互聯機制和開放的 API 策略上，Fortinet 和來自聯盟夥伴的第三方解決方案可藉此蒐集和共用威脅情報，並在偵測到異常行為或惡意軟體時，協調作出回應。

內核網路安全性 - 確保網路安全的第一步就是建立經過強化和主動式的網路內核。Fortinet Security Fabrica 將下述三個基礎的 Fortinet 安全性技術緊密地整合起來，並加入經過專門設計的動態互操作性，實現了上述目的：FortiGate、FortiManager 和 FortiAnalyzer。

外核安全性 - 當網路內核經過強化，並能夠主動監測、分析和關聯威脅行動時，那麼將這一功能擴展到無邊界的網路中就更為至關重要。雲端、BYOD、和物聯網等物件已改變了今天的網路。Fortinet Security Fabric 的下一層級是專注於防護網路外核，包括所有存取方法以及將安全防護延伸到雲端和端點裝置。

延伸安全性 - 安全性也需要延伸到常見的攻擊媒介，如電子郵件和網頁，應主動認真地分析資料和流量以發現未知威脅和零日威脅。這個延伸保護是 Security Fabric 的一個重要功能，包括 Fortinet 進階威脅防護 (ATP) 解決方案，其中包括 FortiSandbox 以及 FortiMail 和 FortiWeb，旨在彌補最常見的惡意軟體和資料丟失方面的媒介防護空白。

全球威脅情報 - Fortinet 的全球威脅研究團隊主動監測全球網路，以尋找、分析和開發針對已知和未知安全性威脅的防護方法。他們的研究針對防火牆、防毒、入侵防護、網頁篩選、電子郵件和反垃圾郵件解決方案提供持續的自動更新。

我們主動式的全球威脅庫可針對網路、內容和應用程式威脅啟用全面的防護，同時我們的安全性研究團隊利用來自多個安全性領域的情報，防禦已知和未知威脅。上述結果將轉換為可執行的即時情報，專門用於在網路罪犯發動攻擊之前，保持防禦。

網路和安全性作業 - Fortinet 的網路安全性和分析工具旨在提供更為全面的方法，蒐集威脅情報、組合和關聯威脅資料，並將相關能力延伸到威脅回應協調，以幫助準備好使用和遵循安全織網的合作夥伴。這一層級的 Fortinet 技術包括 FortiSIEM 和 Fortinet 強化網路裝置套件，例如 FortiAP-U 和 FortiSwitch。

總結

不斷發展的企業網路和過渡到數位化業務模式是當今網路安全面臨的最大挑戰之一。計算和網路連接的顯著趨勢繼續推動著關鍵業務基礎結構、架構和實務內的變化，企業都在尋求創新的網路安全性解決方案，幫助他們適應這種變化。

Fortinet Security Fabric 圍繞可擴展性和安全性的原則進行設計，結合高度的警覺性和可執行的威脅情報，依賴一系列開放的 API 標準，可實現最大的靈活性和整合性。經過妥善部署後，它即可提供當今組織在實體、虛擬和雲端環境所需的協作式有效防護。

如需有關 Fortinet Security Fabric 的更多資訊，請瀏覽我們的 網站。

台灣分公司
台北市內湖區行愛路 176 號 2 樓
電話：02-27961666
傳真：02-27960999

全球總部
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
美國
電話：+1.408.235.7700
www.fortinet.com/sales

EMEA 銷售辦事處
905 rue Albert Einstein
Valbonne
06560, Alpes-Maritimes,
France
電話：+33 4 8987 0500

APAC 銷售辦事處
300 Beach Road 20-01
The Concourse
新加坡 199555
電話：+65.6513.3730

拉丁美洲銷售辦事處
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P.06600
México D.F.
電話：011-52-(55) 5524-8428

2016 年 9 月 20 日