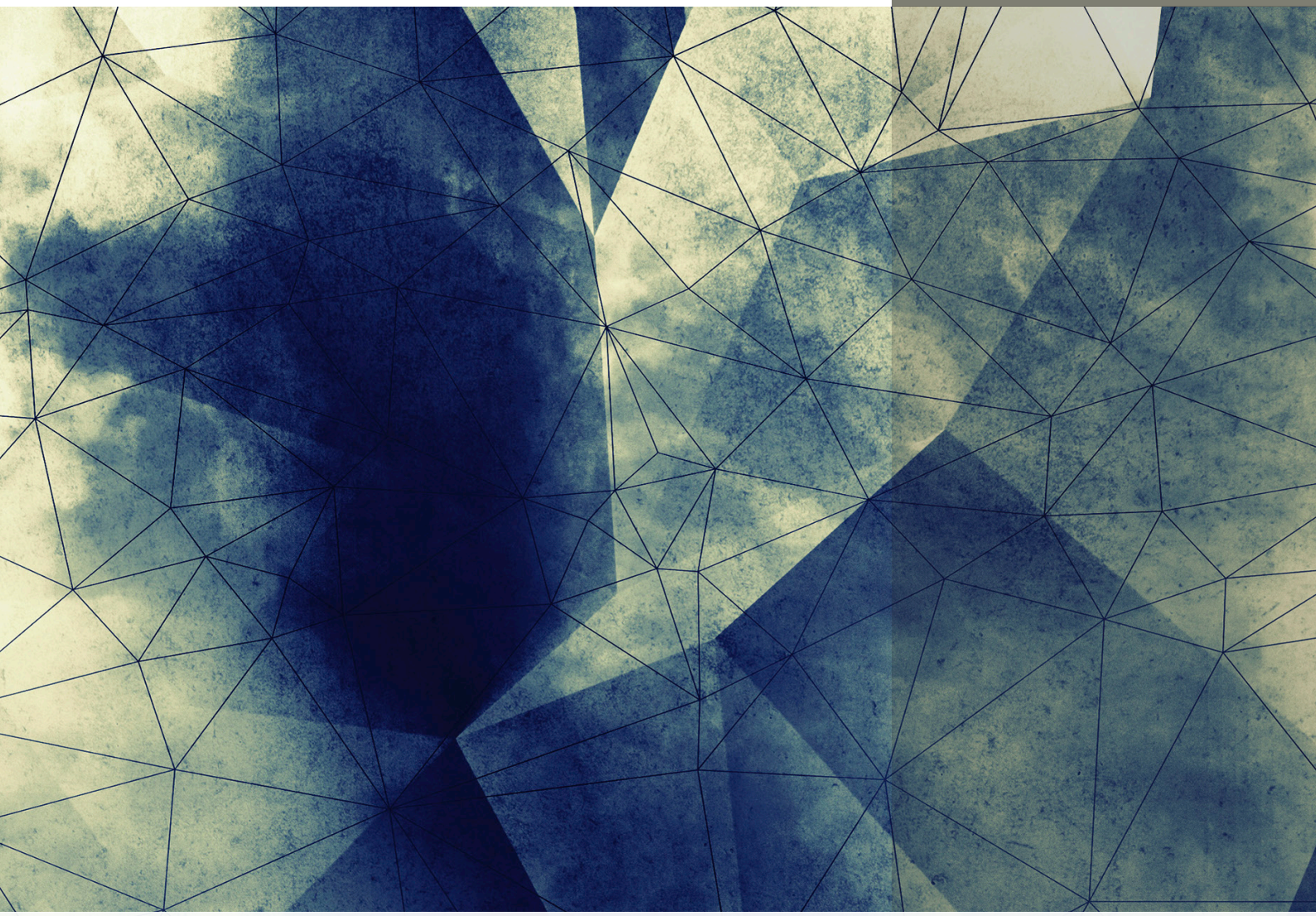
白皮書



保護企業網路安全的新方法
內網安全防火牆

目錄

內容摘要 2
改變的需要 3
一個全面性、自適應式資安策略的基礎 3
將安全系統導入網路深層 4
擺脫線路 – 但未捨棄安全網 6
解決方案管理的優點 6
促進企業轉型 – 人為因素 6
永不妥協的資安防禦 7

內容摘要

關於現今企業在資安威脅活動日益猖獗及複雜的情況下所面臨的挑戰，已有許多的討論和著述。眼見一個接一個的高度機密資料外洩事件以令人憂心的頻率爆發，企業該如何自保？科技是否已無能力應付這些新威脅？

或許我們所見到的是資訊技術的部署考慮不夠周詳的結果，而不是因為技術本身固有的弱點。如果是這樣的話，那麼這應該被視為一記警鐘，喚醒企業重新思考他們的資安措施。

保護網路安全的方法不止一種，不同的組織會根據其需要及預算採取不同的做法。例如對銀行和零售業者來說，合規性（如 PCI-DSS）是一個關鍵要素。雖然 PCI-DSS 的合規性是這類垂直產業的必然考量要素，不過資安措施不應止於滿足一般性的要求。此外，還有其它組織採取更進一步的行動，透過執行風險評估及根據發生機率分配安全預算。此做法除了確保合規之外，也考慮到企業幾乎每天都須應付的新變化以致於對年度風險評估的準確性存疑的潛在風險。最後是部署來自不同廠商主要產品的「單點產品」，此做法的前提是每項產品均為其同級中的最佳選擇。儘管這個「最佳品種」組合被認為是最周全的做法，管理如此先進、繁複的產品組合的成本及複雜性的增加卻也是個非常現實的問題。

本文的目的在於介紹一個實施網路安全的新概念，此概念以三個界定原則為基礎：

- **全面性 – 從資料中心至終端及更遠位置的端對端**策略，可透過整合式的預防、偵測及修復能力應付威脅
- **協作性 – 解決方案元件的協同運作**與網路能力結合，以收集及分享即時的威脅情報
- **轉型 – 將**企業網路從一組盒子變成一個結合技術與人類知識的平台

與此同時，企業所面臨的另一個問題是定義明確的網路外圍防線遭受侵蝕。日新月異的技術及企業使用技術的方式，形成了一個無邊界的攻擊面，進而提高駭客成功攻擊及資料外洩的可能性。

Fortinet 認為現在正是改變對網路安全性的認知、更重要的是改變其實踐方式的時機。當今的網路在企業的經營策略上所扮演的角色比以往重要許多。在複雜且不斷變化的威脅環境下不對此關鍵資產的安全提供保障，是大多數組織無法承擔得起的風險。

改變的需要

網路安全性為何迅速變得重要起來？過去 20 年間，許多企業經歷了轉型變革，甚至在技術的運用下創造出以往無法想像的全新業務模式。技術徹底改變了企業 – 製成品已不再是最重要的一塊拼圖。取而代之的是資訊 – 海量的數據可讓企業一次又一次地分析，以推動業務發展。資料中心及網站已從成本中心搖身一變成為關鍵的商業資產。但是這一切須仰賴一個健全的網路才能發揮效用。如下圖所示，如果客戶資料是金字塔的塔尖，則其下的網路便是是根基（圖 1）。問題是這個根基是否有太多的裂縫而使客戶資料處於危險。

由於企業擴展是網路成長的主要驅動力，網路的首要條件便是支援企業。安全系統雖然在一定程度上存在，但經常是被動地將幾個基本功能「綑綁」至網路上的權宜之計。然而隨著時間的推移，這種安全模式已被證明是不足夠的。沒有充足的安全措施、太多可入侵的漏洞以及惡意軟體製作者的無限創造力形成了一場完美的風暴，將企業攻得措手不及。

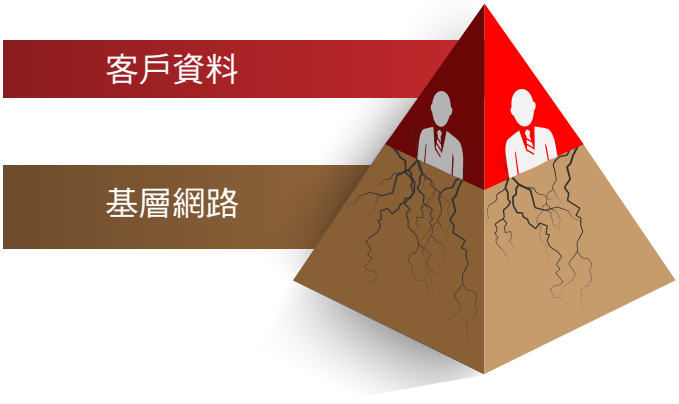


圖 1 – 企業的進化

一個全面性、自適應式資安策略的基礎

沒有任何安全結構能夠百密無一疏地將所有惡意軟體阻隔在網路外。因此，目標在於盡可能阻擋最多的惡意軟體進入網路、盡快偵測出任何入侵網路的動作，並確保遭受攻擊時能妥善保護最關鍵的資產。那麼應如何實現這些目標呢？

在 Fortinet，這首先從安全系統應內建於網路基礎架構中的概念開始做起。此做法可自動減少、甚至消除兩個層級之間的間隙，並開始關閉駭客的機會窗口。然而僅僅運用技術，即使緊密整合至網絡基礎架構中，也不足以防禦現今的威脅環境。這些部署在核心、分支機構或桌上型電腦上的技術必須在一個共同基礎上以單一解決方案的形式交互運作。

Fortinet 可將適當的技術配置於整個網路中的適當位置 – FortiGate 下一代防火牆，FortiWeb Web 應用防火牆（WAF）、FortiMail 安全電子郵件閘道器（SEG），FortiSandbox 網路沙箱及 FortiClient 終端保護（EPP）客戶端軟體（圖2）。Fortinet 的做法與傳統做法的不同點在於這些技術皆可獲得 Fortinet FortiGuard Labs 實驗室的威脅情報支援。這些產品都附有一個或以上運作中的安全服務，有些是其功能操作的必備工具（例如 SEG 附有防垃圾郵件服務），另一些則是為了提高其安全系統的效用性而設計（例如 FortiGate 的防病毒或入侵防禦系統）。相較於傳統的片段式單點解決方案，各家廠商將提供各自的威脅情報。問題是各產品的安全效力參差不齊，因此會形成可被入侵的漏洞。由於攻擊向量不僅一個，被防火牆阻隔的惡意軟體也可能從被侵入的網站或以釣魚郵件的附件或網址的形式成功進入網路。Fortinet 資安策略中的不同安全服務持續由 FortiGuard Labs 更新及同步化，以防止產品之間形成任何間隙。FortiGuard Labs 是 Fortinet 生態系統的核心，負責接收來自世界各地的數百萬個感測器及其它來源所接收的即時威脅情報。除了這些資訊之外，該網路專家團隊還進行先進威脅研究及尋找「零時差」漏洞作為輔助。FortiGuard Labs 實驗室輸出的資訊可為 Fortinet 設備上執行的不同服務提供持續更新 – 藉由單一來源的資訊更新消除不同設備之間的間隙。

為了進一步消除任何可能的間隙，這些產品的設計是作為單一解決方案的元素協同運作，為網路提供防止惡意軟體進入網路的能力、偵測出入侵網路的惡意軟體、提供重要的緩解功能以盡可能減少攻擊帶來的任何傷害，以及持續更新解決方案以防患於未來。

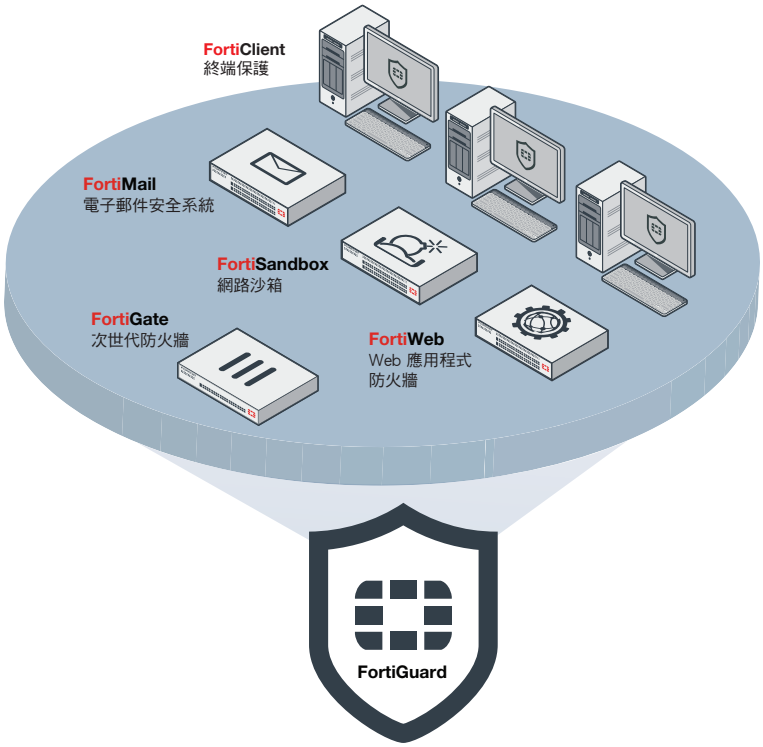


圖 2 – 涵蓋整個網路的安全性

Fortinet 本身的沙箱技術可使安全元件的整合更為緊密。在此，一個必須考量的重點是沙箱如何與網路中的其它安全元件互動。土法煉鋼的做法是讓沙箱持續尋找惡意軟體樣本，然後對找到的所有樣本進行分析。不過，此做法的問題在於太耗時。從惡意軟體入侵到沙箱偵測出來時可能已經過了數小時，而惡意軟體早已利用這段時間散佈至整個網路。Fortinet 的做法是將沙箱與其它網路技術緊密整合。組成防護層的技術可發揮類似初級濾網的功能，阻擋一大部份的惡意軟體進入網路。然後將可疑的樣本轉到沙箱上進行分析。如果找到惡意的樣本，沙箱會傳達給解決方案的其它元件，以便採取具體行動，展開初步的緩解措施。

透過使用專為協同運作而設計的不同技術並在即時威脅情報的支援下，Fortinet 解決方案可為網路防禦攻擊的能力提供傳統防禦措施所無法提供的深度。

將安全系統導入網路深層

雖然在好萊塢電影中，網路攻擊總是發生在想像中那種佈滿電腦的資料中心裡，在現實生活中，攻擊卻可能在網路中的任何一處發生。 網路應該被視為一系列的同心圓，以網路的核心為中心點（圖 3）。由於成本上的考量，安全系統一般集中於核心。隨著圓圈從核心到分支機構、再到個別的桌上型電腦等持續向外擴展，潛在的攻擊點數量也呈指數增加。結果即是，離開網路核心越遠，網路入侵未被偵測到的可能性就越大。

圖 3 – 日益增加的威脅風險

為了解決這個漏洞，常見的做法是在整個網路內部署安全系統。部署於分支機構和遠程位置、企業園區的邊緣、雲端資源的登入點及資料中心裡的防火牆，可有效地將網路區隔成安全的網格（圖4）。當此策略將不同廠牌的產品混合使用時，例如為資料中心選擇一個廠牌、園區選擇另一個廠牌，然後為遠程站點選擇第三個廠牌，可能會讓

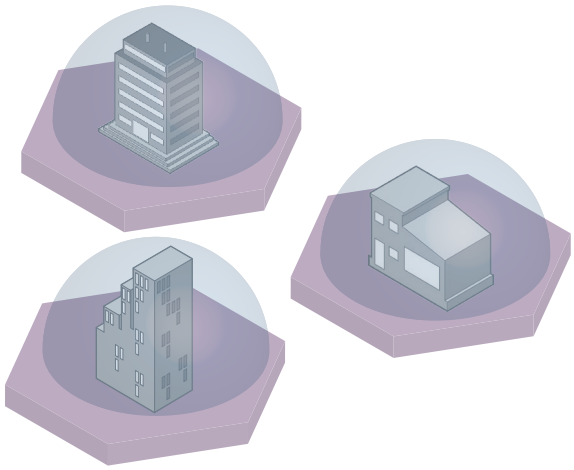


圖 4 – 已區隔，但不安全

一切亂套。雖然每個產品都可各自發揮預期的功能，但它們基本上都是各自獨立的孤島，使得管理整體網路的安全政策變得困難又費時。

而 Fortinet 能夠透過 FortiOS 克服這些問題，FortiOS 是所有 FortiGate 的通用操作系統。無論部署於網路中任何位置，分佈在整個網路中的 FortiOS 的通用功能可為企業提供一個雙贏的環境 – 透過內部區隔策略以及貫穿整個網路的統一安全政策提供一個更安全的網路。FortiOS 也是 FortiGate 支援的所有安全服務的引擎，可確保整體網路都受到同等的保護（圖 5）。

但此區隔策略仍著重於防守網路外圍，而無法阻止能夠進入網路而未被發現的駭客，尤其如果該駭客使用有效、但已被侵佔的登入憑證。沙箱是這個問題的一個可能對策，但在駭客將惡意軟體植入網路之前，沒有什麼可以停止他們在網路中的行動 – 直到現在。

Fortinet 認為現在是將此區隔概念延伸至網路內部的時候。雖然網路早已開始實行區隔的概念，不過是為了網路連線的目的，並無法阻止惡意軟體或駭客在網路四處自由擴散。這個問題的解決方案便是內網安全防火牆。

內網安全防火牆背後的概念是使用一個企業級的防火牆部署於網路內部盡可能接近用戶及應用程式的位置。這包括企業園區及資料中心。與用戶及應用程式之間的近距離是決定水平擴散風險減少程度的關鍵。另一個關鍵是安全政策與用戶身份之間的配適。將安全政策與用戶身份連接，可利於建立一個政策防止用戶進入與他們正常工作職務不相關的網路部分。例如，財務部虛擬區域網路（VLAN）上的用戶嘗試進入工程開發部 VLAN。實行內網安全防火牆之後，試圖從最初入侵點 – 在此例中為財務部門 – 移動至工程開發部網路的駭客將被防火牆阻擋，同時會發出警報告知發生了什麼事（圖 6）。

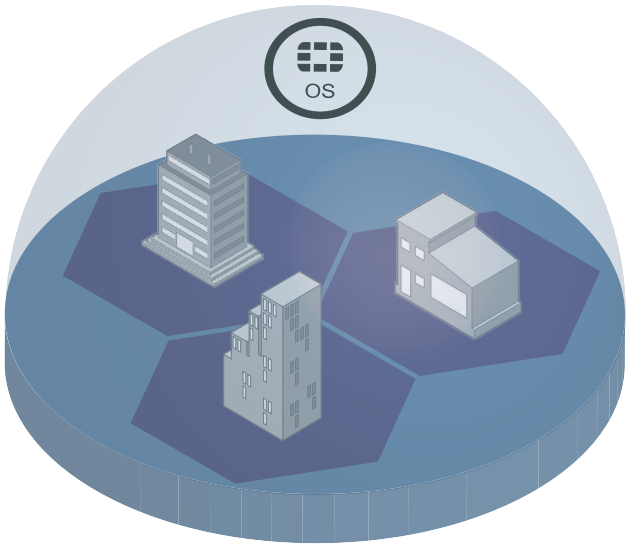


圖 5 – 受到 FortiOs 的保護

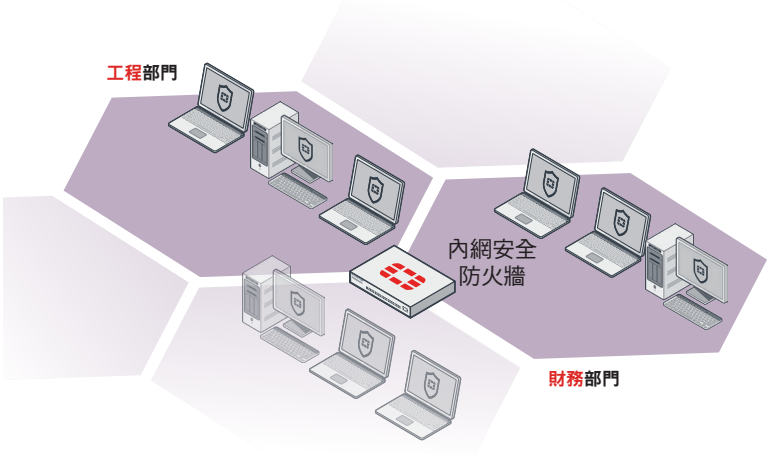


圖 6 – 解決方案：內網安全防火牆

內網安全防火牆引發了一次從多功能安全性進化至多層次安全性的變革，因此需要高速的安全設備。Fortinet 憑藉其 FortiASIC 技術而擁有一個強大的差異化優勢，使我們能以內部網路的 10、40 及 100 千兆位線速提供深層安全性。Fortinet 的內網安全防火牆可由內至外提供持續的網路可見度與保護，以縮短漏洞空窗期及減少潛在的損害。

擺脫線路 – 但未捨棄安全網

在當今的現代企業裡，無論是為了內部使用或提供更佳的客戶體驗，無線技術已從一個方便的功能變成一項「必不可少」的工具。但企業的挑戰是如何在不影響安全的前提下提供一個統一的存取環境。傳統的分支機構無線網路是一種層疊結構 – 這表示無線網路與其底下的網路基礎架構是各自獨立運作的。無線網路雖然也以 Wi-Fi Protected Access（無線保護存取，包括 WPA 及 WPA2）等存取控制的形式提供安全性，它與網路的安全系統卻並不相同。無線網路需要的是一個所有用戶無論使用何種存取方式均可通用的安全框架。

在 Fortinet 的安全存取架構中，無線網路是 FortiGate 本身的延伸。除了典型的無線網路 – WPA – 的存取控制與安全功能之外，所有網路用戶都須接受相同的身份驗證及政策約束。身份驗證可由 FortiGate 在本機執行，或透過 RADIUS 或 Active Directory 等外部系統進行。此外也可採取雙重驗證（2FA）措施，以盡可能減少來自有效、但已被侵佔的登入憑證的風險。用戶的身份一旦確認及驗證之後，只能存取其政策中定義的網路資源。由於用戶須通過 FortiGate 登入網路，惡意軟體進入網路的可能性也將顯著減至最低。

端對端的安全性、端對端的控制

除了所部署的解決方案各元件之間的協同運作之外，採取積極安全措施的另一個關鍵要素是集中化的安全管理與分析。由於網路上的問題狀況極其廣泛，需要採用全面性的工具幫助正確設定解決方案中的不同元件，釐清問題並呈現清晰的網路視野。Fortinet 的解決方案包含單一虛擬平台式的網路管理系統 FortiManager，以簡單、直接的程序進行個別產品的設定、定義策略導向的供給、更新管理及端對端網路監控。

FortiManager 的圖形用戶介面（GUI） 設計，使網路管理員只需點擊幾下即可深入鑽取細節，了解警報及網路上發生的其他事件。安裝及設定好網路之後，下一個目標便是了解網路的當前狀況，並將一系列的警報及事件轉換成清晰的網路工作站視野。FortiManager 可與 FortiAnalyzer 完美無縫地整合，以提供有關網路資安事件的深度搜尋、分析、優先排序及報告。

促進企業轉型 – 人為因素

實施及維持網路安全系統並非一朝一夕之事。企業應持續測試他們的安全解決方案，並充分善用其技術夥伴可提供的專業服務。並非所有的企業都擁有全方位的安全技術知識與技能，可確保正確設定及部署所有安全技術。漏洞測試與評估、組態設定審查及訓練都是正確部署網路中的技術及確保無「後門」等著被滲透所能採取的措施。事件回應是企業可以利用及借助技術供應商的技能與知識來輔助其內部員工的另一項服務。Fortinet 與其客戶緊密合作提供前述服務，並為因應瞬息萬變的市場推出新的服務。

另外，Fortinet 也提供一系列集中於幾個特定領域的頂級支援服務，以提高企業可獲取的價值 - 積極應對、持續改進與協同合作。這些服務如專門的技術客戶經理（TAM）等，可加強服務等級協議與升級及實驗室的預置作業，確保 Fortinet 的解決方案能滿足企業在整個生命週期中的需求。

永不妥協的資安防禦

考慮到當今的企業及推動其發展的技術之間的關係，著眼於保護 IT 基礎設施的安全應該是一個基本要件。但有太多企業仍將資安系統視為一項令人存疑的費用，而非戰略性的投資。等到資料外洩發生後再檢查其當前安全態勢的企業，就好比在房子遭人破門而入之後才將大門鎖緊。

Fortinet 有兩項目標 – 站在前沿致力改變對企業安全的心態，以及成為組織可信賴的合作夥伴，指引他們渡過此變革階段。

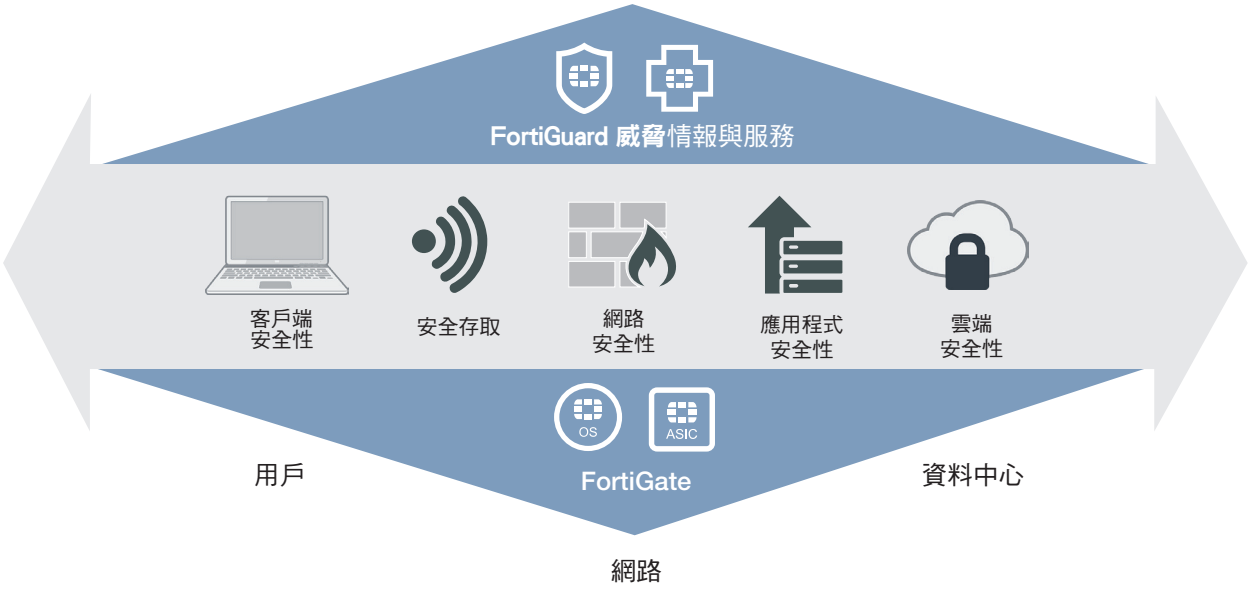
> 網路必須從整體的角度審視，即可看出它是一個單獨的實體。在適當的位置配置適當的技術，才能提高網路偵測攻擊的能力並在整個威脅的生命週期中保衛自己。

為了強化威脅的偵測能力，必須利用持續且相關的威脅情報支援技術，讓技術能充分善用這些情報採取具體的行動措施及提升其安全效用。

Fortinet 憑藉其產品陣容的廣度與深度 – 專為網路各功能領域設計的產品以及為協同運作而設計的產品 – 實現這個全新的網路安全概念。回應不僅只是一個本機動作，因為 Fortinet 解決方案的設計旨在於協同工作以及自動、積極地採取應對措施。每一個動作都會自動且一致地傳回威脅情報生態系統，以強化整體的解決方案。

最後一塊拼圖便是人類的智慧與人工介入，為技術與企業自身人力資源提供支援。Fortinet 及企業結合雙方人員的專業知識，共同合作消除組織內的薄弱環節，進而提高企業的整體防禦能力。

企業每天面對的威脅不論是數量或複雜程度都在持續增加，因此必須改變對網路安全性的看法。Fortinet 非常樂意與企業合作改造及擴充其網路安全措施，從被動的做法轉換成自適應、全面及協同合作的做法，並結合最頂尖的技術與人力。



無縫
完美無縫的端對端、一致的威脅防禦態勢

智慧
由內至外的智慧防護，提供橫跨攻擊面的完整可見度

強大
滿足今日至未來需求的動力與性能

FORTINET®

NetFOS 逸盈科技
www.netfos.com.tw

台 北
台北市八德路四段760號7樓
TEL: +886 2 6636-8889
FAX: +886 2 6638-9998

新 竹
新竹縣竹北市高鐵二路32號13樓之5
TEL: +886 3 621-5128
FAX: +886 3 668-4058

台 中
台中市文心路四段696號7樓之2
TEL: +886 4 3606-8999
FAX: +886 4 3602-0999

高 雄
高雄市裕誠路392號10樓之2
TEL: +886 7 862-8889
FAX: +886 7 862-9998

---

www.fortinet.com

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

歐洲、中東和非洲
銷售辦事處
905 rue Albert Einstein
06560, Sophia Antipolis,
France
電話：+33.4.8987.0500

亞太銷售辦事處
300 Beach Road 20-01
The Concourse
Singapore 199555
電話：+65.6513.3730

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

Copyright © 2016 Fortinet, Inc. 著作權所有。保留一切權利。Fortinet®、FortiGate®、FortiCare®、FortiGuard® 和某些其他標誌為 Fortinet Inc. 的註冊商標，此處提及的其他 Fortinet 名稱亦為 Fortinet 的註冊及/或普通法商標。其他所有產品或公司名稱可能是其個別所有者的商標。本文所載的效能和其他指標是在理想條件下取得的內部實驗室測試結果，實際效能及其他結果可能有所差異。網路變數、相異的網路環境及其他條件均可能影響效能結果。本文中的任何內容均不代表 Fortinet 所作出之具約束力的承諾，並且除 Fortinet 訂立之書面合約所載的擔保條件外，Fortinet 在此免除一切明示或暗示的擔保條件。前述書面合約必須由 Fortinet 的總法律顧問與購買方共同簽署並明確擔保指定產品將按照已確立的效能指標運作，在此類情況下，Fortinet 的擔保範圍僅限於此類具約束力之書面合約所載明的具體效能指標。為明確釐清，任何此類擔保將限於與 Fortinet 內部實驗室測試相同理想條件下的效能。與此有關的任何約定、聲明或保證，無論明示或暗示，Fortinet 概不負責。Fortinet 保留不另行通知隨時變更、修改、傳輸或以其他方式修訂本發佈內容的權利，如有任何歧義，概以最新版本的發佈內容為準。