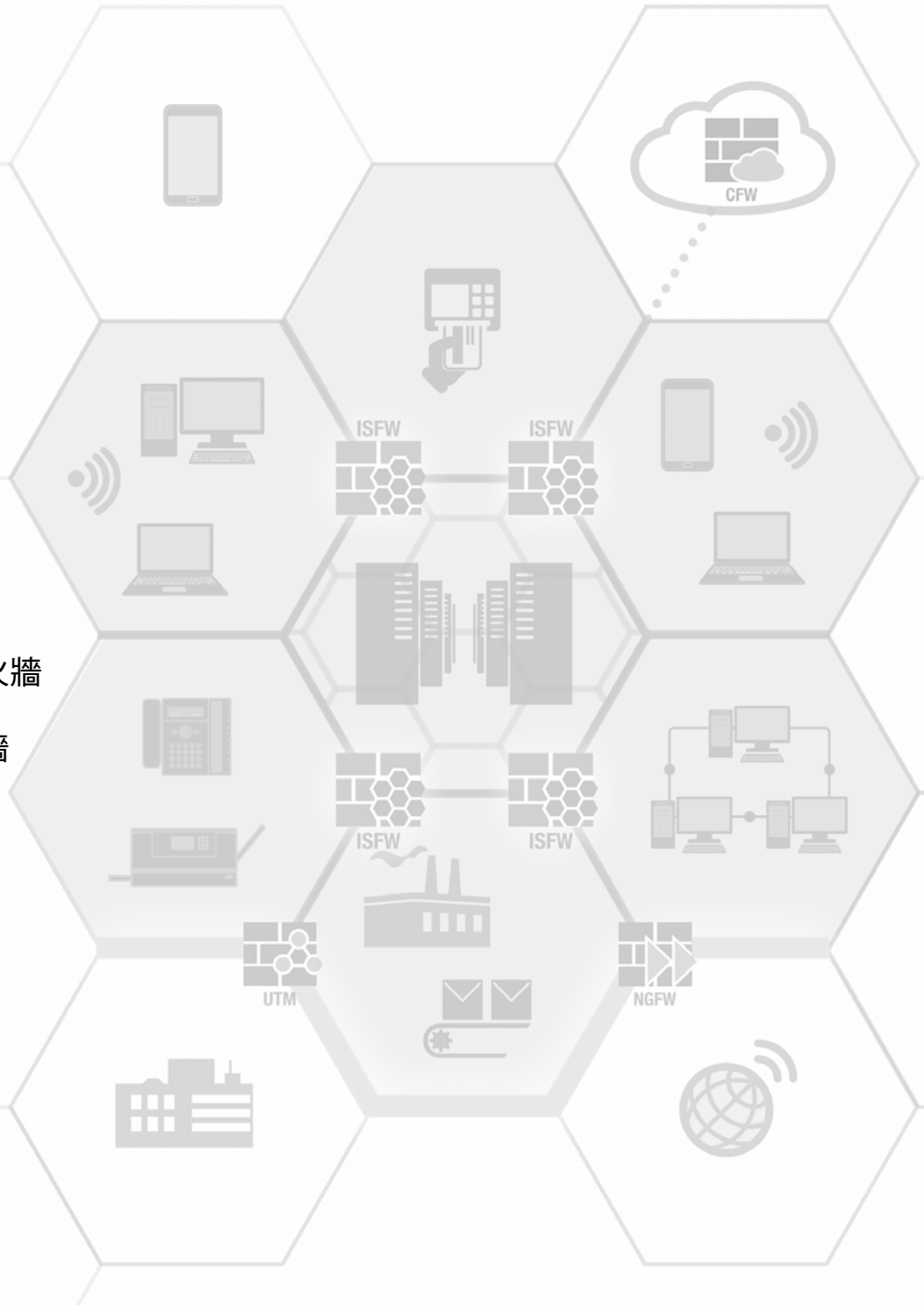

FORTINET
安全性
由內至外滴水不漏
最新的入侵防禦策略
永不妥協的資安防禦

目錄



簡介

資料外洩問題已經從資訊長或資訊安全長的責任範疇提升至執行長的範疇。許多企業的董事會及其它外部機構都紛紛提出不少個關鍵的問題：公司已做好哪些抵禦進階攻擊或資料外洩的應變準備？您將採取哪些策略來應付網路基礎架構被入侵時的突發狀況？

現在，這些問題極具重要的戰略意義。執行長和董事會已將討論升級至計算風險及建立有效的解決方案，為許多人認為無可倖免的危機做好準備。在本文中，我們將討論為何傳統的周邊防護策略已不敷使用，以及為何在您整個企業部署專用的「內網安全防火牆」，將有助於提高您的網路在面對今日的進階威脅所需的回應與應變能力。

01

周邊防線已不敷所需

還在不久之前，網際網路的存取仍能做到非常嚴密的管控。一個典型的企業網路可能是由若干個連接至網際網路的備援連結組成，而所有流量都會經過一個點。因此，企業可以在網際網路及其所有罪惡來源與安全的內部網路之間部署一道周邊防火牆。但時至今日，情況已經明顯不同。隨著各種網路裝置的急速發展、自帶設備蔚成風潮、雲端與雲端技術的運用以及物聯網的出現，所構成的攻擊面已經無法抵擋攻擊者的入侵。僅在您的網路周邊設立一道防火牆並抱著僥倖的心理是不夠的。這種做法也不再有效。現今的威脅持續不斷地演化與擴增，因此您的網路防禦系統也必須持續調整，以面對這個新現實。

如今，公司在網路安全性方面的花費比以往都高出許多。您可能會感到納悶，那為何資料外洩仍然會發生。企業通常將大部分的安全支出集中於他們的資料中心和核心網路。畢竟，公司絕大部分的機密資料都在這裡！但是，攻擊者是聰明狡詐的。他們不再將所有精力和資源集中在資料中心，至少不會直接入侵。現在的攻擊者將相當多的時間花費在入侵終端及核心網路以外的其它系統，他們會先攻擊一位終端用戶，盜用其憑證，然後再利用登入權限在網路中側向移動。通常他們會探索及標定靠近其最初進入點的裝置和系統，再設法攻佔其它系統、提高他們的權限、從內部系統中未及更新的漏洞乘虛而入、植入更多惡意程式並竊取資料。一旦攻擊者集合所有竊取的資訊之後，他們會利用之前的調查找一個隱密的方式，帶著所有戰利品潛逃出去。

而當攻擊者成功侵入時會如何？從多個來源的各種分析都認為，現在可能需要很長的時間才會發現系統中的一個漏洞及遏阻攻擊者的行為。您的企業可能須為此付出慘痛的代價，包括取證、補救、法律費用及額外的防禦措施等都須耗費龐大的資金。還有對貴企業的聲譽及品牌造成的影響呢？這可能已無法估量。

為什麼現有的防火牆措施已不敷所需？雖然攻擊者能夠利用更多的技術避開周邊防線，但在許多情況下，他們並不需要這麼做。正如我們前面提到的，比起從前，現在已經有更多的方法能侵入一個網路。這些方法都有能力越過周邊的防護機制。

您必須體認，在現今的資安策略中，有效的安全措施在保護周邊的同時也必須建構一套內部防禦系統。在今天，監控您的內部流量可以說與監控來自網際網路的流量同等重要。那麼，現今的安全團隊該如何加強他們的防禦系統呢？

02
新的防禦策略：內網防火牆

作為一個有效之防禦策略的一部分，您必須能有效地將您的網路分割成更小的「區塊」，使負責不同職務的員工團隊各自獨立運作。例如，您的研發團隊可能沒有理由需要存取與會計有關的系統，而您的人力資源系統應該也不需要連接至財務部門。

深度防禦 並不是個新名詞，許多企業或多或少都有採用這項策略。深度防禦可讓您將多個安全控制系統佈署於網路各處，以在攻擊週期中的某個時間點偵測到某個事件。而內網安全防火牆便可建立「區塊」及監測異常的網路流量，更進一步延伸深度防禦的概念。

大多數的外圍防護解決方案在檢查對外流量（如有此功能）方面成效也不佳。舊式系統往往假設您的網路內部是安全或無害的，因此主要著重於保護內部免遭外部惡意份子的侵襲。即使是能夠提供一定的對外流量檢查功能的防火牆，當工作負載量增加時也往往應付不來，進而造成嚴重的瓶頸或效能問題。

內網安全防火牆如何偵測出周邊防火牆偵測不到的活動？必須了解的一點是，內網安全防火牆並不是為了偵測外圍系統偵測不到的活動而設計的。您的內網安全防火牆應將具體的政策納入設計考量，讓您的用戶能夠存取他們該存取的內容，同時延緩或完全禁止他們存取您網路的其它區塊。因此，如有攻擊者侵入您的某位會計團隊成員的終端時，他們應該無法在網路上四處移動及進入您的銷售點或電子商務控制系統。您的內網安全防火牆應該能偵測出這些試圖存取用戶常規活動以外系統的動作，並發出相應的警告。除此之外，您的內網安全防火牆還能識別及封鎖來自惡意軟體、殭屍網路或其它成功突破您的周邊防線的惡意活動威脅。例如 ZeroAccess 便是一個以「話多」的特性聞名的殭屍網路。它經常會搜尋其它殭屍網路，與其溝通並接收指令。您的內網安全防火牆由於位置接近受感染的終端，因此具備偵測該傳播程式的優勢條件，也能比周邊防禦設備更快向您的安全團隊發出警報。

內網安全防火牆的部署位置愈接近網路存取層愈好，因為這可讓您最全面存取您的網路資產及大部分的內部流量。採取此方式部署內網安全防火牆，例如貫穿所有從存取層至核心層及分送層的上傳連結，您將可獲得該所有內部流量的可見度。您可以快速部署您的內網安全防火牆，就類似部署交換器一樣，也就是我們所謂的*虛擬線路模式*。這不僅可加快部署速度，也可避免設定傳統外圍設備的高度複雜性。您不需要重新設定網際網路協定、閘道器或其它資產，並可獲得對您整個網路中移動的流量的深入可見度。

03 如何選擇內網安全防火牆

直到最近，許多公司一直不太願意在他們的網路基礎架構中添加例如內網安全防火牆的多一層防線。根據近期的統計調查顯示，進出您的資料中心的流量有多達四分之三現在都在您的網路基礎架構中。擁有能夠監測該內部流量的傳輸率、處理能力及埠密度的防火牆即使存在，成本也高得驚人。除了部署這些裝置所造成的干擾之外，還會加重您已經工作超載的資安人員的管理負擔，使企業無不選擇將資源投注在其他方法上。

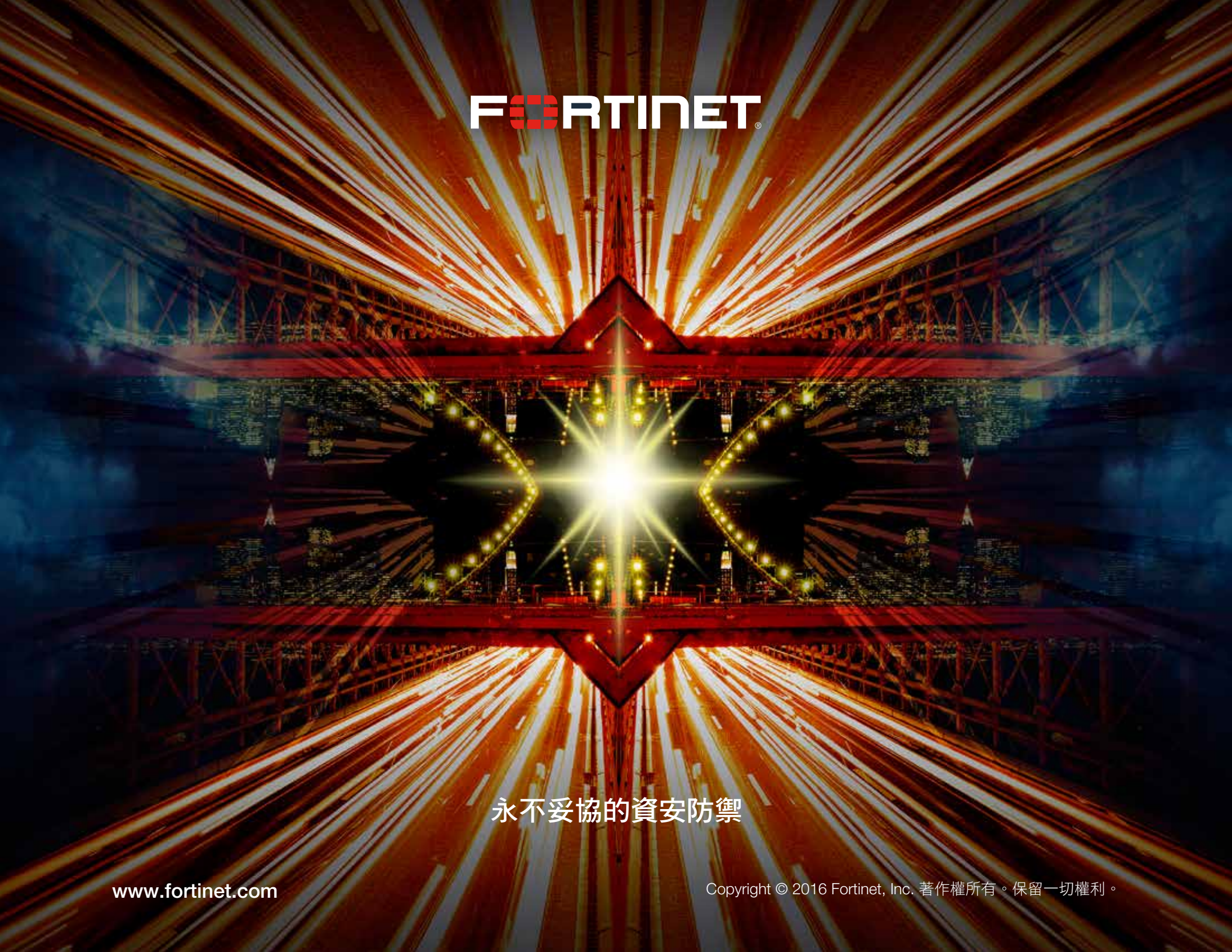
如今，性能可說是選擇一個內網安全防火牆的最重要決定因素。即使是無線網路也已接近十億位元（Gigabit）級的真實世界傳輸率；十億位元也是桌上型系統的常規，而非特例。為滿足這些速度要求，您必須擁有一個埠密度及速度足以應付前述網路需求的內網安全防火牆。您的安全基礎架構也必須能夠以線速或接近線速的速度運作。用戶將無法接受任何性能上的降低或退化。現有的或已除役的防火牆如果運作時會產生瓶頸，則再利用該防火牆並非有效率的做法。

另一項決策關鍵在於防火牆與您現有安全基礎架構的整合。是否需要重新訓練您的員工使用該防火牆？他們能否將使用周邊裝置所獲取的知識與技能延伸至內網安全防火牆？最後，必須將有形與無形的部署成本考慮在內。您能否迅速且有效率地部署您的內網安全防火牆？將一個內網安全防火牆設置到位，對網路的干擾程度會有多大？

結論

分隔您的網路其實並非新概念。但傳統的分隔模式採用的是以網路連線技術為基礎、成效不彰的措施。對技術高明的攻擊者來說，這只不過是另一個減速丘。

您必須部署路障才能阻隔攻擊者的攻勢。如今隨著防火牆性能的進化，我們可以實現新的分隔策略：不僅能抵禦來自您網路外部的威脅，也能防範網路內部出現的威脅。現今的高性能內網安全防火牆可助您建構一個有效的內部分隔策略，在保護重要資產的同時不需犧牲營運表現或對您的業務造成干擾。



www.fortinet.com