

中小企業防護指南

縮小防護落差並捍衛您的
企業未來

防護落差

對於中小企業來說，電腦已經是不可或缺的生財工具。儘管 IT 技術不斷出現各種全新的風險與管理難題，大多數企業主管仍舊願意在大致瞭解相關風險後，盡可能地加以解決。而這通常意味著需要採用網路防火牆、新增防毒，甚至是垃圾郵件過濾解決方案，並建置某種形式的備份排程。

無可否認地，要同時兼顧業務與最新的防護絕對不是一件容易的事。最新的研究對此落差敘述如下：最近一項調查¹ 顯示，33% 的中小企業甚至沒有基本的防毒能力，而 47% 的企業則是無法備份桌上型電腦，剩下的 20% 則根本沒有對伺服器進行任何備份作業。

隨著風險不斷增加，企業的防護問題也跟著惡化。越來越複雜的威脅與攻擊模式開始常態性發生，有些甚至鎖定個別企業發動攻勢。資料的價值與資料遺失成本同時上升。隨著無線網路、行動運算裝置、工作場所中的 Mac OS® 與 Linux® 機器與網路閘道及伺服器硬體陸續加入基礎架構中，技術環境也跟著改變，但是這些新增項目卻沒有一樣受到基本的防護。

個別的「單一功能產品」可能可以滿足特定需求，但卻無法有效整合，因為：

- 個別產品的重複性會造成時間、人力與金錢上的浪費
- 落差與防護涵蓋範圍不均的問題導致重要資產與資訊陷於風險之中
- 解決方案管理作業佔據了許多可用來增加更多企業價值的工作技能與時間

為了縮小這些防護落差，中小企業需要一套可靠、完整且相容的防護機制，搭配規模適中的設計以便輕鬆安裝、設定與使用，而此機制必須來自可信賴的廠商。

評估您的防護涵蓋範圍

右側文字框中的「防護階段」勾勒出許多中小企業從低成本解決方案過渡到成熟、可擴充的安全與資料防護基礎架構時必經的過程。儘管許多中小企業已經進階到使用單一領導廠商所提供的第 1 階段相容性解決方案，更多企業還是希望維持原本的第 0 階段防護水準，盡量以硬體、作業系統或是 ISP 服務提供的各項解決方案湊合著使用，並倚賴自行建構的備份與復原方法。以下各章節將概要說明這些初階防護方法可能遺留的防護後遺症，並點出這些方法所導致的幾項管理難題。

防護階段

本指南說明中小企業的四大防護階段：

第 0 階段—DIY 式多廠商防護，亦即將電腦、網際網路存取服務以及外接式硬碟隨附的各種單一功能解決方案組合在一起。這種作法可能會造成防護上的落差，而且也難以管理。

第 1 階段—視需要添購來自單一廠商的各種單一功能解決方案並加以組合運用。這種作法可能會造成重複的代理程式、流程與主控台，進而影響效能並讓管理更形複雜。

第 2 階段—採用專為中小企業需求所設計的單一廠商套裝軟體。合併且簡化的代理程式、流程與主控台可提升效能與管理能力。

第 3 階段—採用進階的單一廠商解決方案以延伸各項套裝軟體之功能，以符合特定企業需求，並由廠商的技術合作夥伴加以客製化，以便完全吻合企業需求。

¹ Applied Research - West, Inc. *Storage and Security in SMBs: 2009 調查結果* (Cupertino, CA: Symantec Corp. March, 2009), http://eval.symantec.com/mktginfo/enterprise/articles/b-storage_and_security_in_smb_03-2009.en-us.pdf.

端點安全

技術上而言，「端點」指的是 TCP/IP 或其他傳輸層連線的來源或目的地。實際上，端點指的就是負責收發資訊的伺服器、桌上型電腦、筆記型電腦與行動裝置。由於裝置與資訊跨越網路邊界的機會越來越普遍，例如員工可能在機場或咖啡廳上網、約聘員工帶自己的筆記型電腦來使用，或者竊賊嘗試從貴公司的停車場建立 WiFi 連線等，因此絕對有必要確保端點的安全。在抵禦全方位攻擊行為上，周邊安全性仍有其重要之處，但還不足夠。

第 1 階段的端點安全整合了防毒、防火牆、入侵防禦與其他防護機制來減輕系統、使用者與管理上的負擔。

第 2 階段的防護安全性則更上層樓，將多種解決方案融合為易於管理的單一解決方案：

- 其中**防毒和防間諜**程式則是大家最熟悉的端點防護形式。今日的最佳解決方案能夠運用縱深防護機制來抵禦隱匿的“rootkit”惡意程式、使用更少的系統資源來運作並以前所未見的效率滿足使用者對效能的需求。
- 屬於主機型防火牆的**網路威脅防護**機制藉由網路流量規則（而非尋找過去的攻擊特徵）以保護網路安全。此類型的端點防護機制可依據原始設計用途來攔截各種威脅，就算碰到從未見過的威脅型態也能應付自如。
- **主動式威脅防護**機制透過用戶端規則引擎來運作，即使面對全新的威脅型態也能發揮最後一道防線的效力。
- **單一代理程式與單一主控台管理**功能可有效管理各項運算負載與管理負擔，只要在最基本的時間與資源條件下就能發揮安全技術的最佳效能。

第 3 階段的端點安全透過額外的解決方案來強化第 2 階段防護效能，藉此符合更多特殊需求，例如：

- 軟體或硬體裝置格式的**網路存取控管**機制可以維持並強制執行網路權限的授予或限制政策，無需顧慮端點存取資源的方式。
- **端點的防止資料外洩**機制可掃描入埠與離埠的通訊，以找出社會安全碼或信用卡號之類的重要資料，並強制執行相關政策以限制個別訊息可包含或是員工可傳送的重要資料數量。
- **特殊裝置的防護**機制範圍則涵蓋今日異質化網路中越來越常見的 Mac OS、Linux 與行動裝置。

郵件安全

垃圾郵件不只浪費信箱容量而且惹人厭，不過，ISP 業者在第 0 階段的垃圾郵件過濾防護解決方案能減緩急迫性，因此受到許多中小企業的青睞。第 1 階段的解決方案除了以上 ISP 所提供的產品項目之外，還提供了更有效的過濾解決方案，而且只需要佔用到系統管理員一點點時間。

但是 ISP 業者的防護機制對於鎖定個別公司或人員所發動的攻擊卻束手無策。即使是最佳的第 1 階段垃圾郵件過濾解決方案都不是專門設計來防止不當且存在法律風險的內容、機密資訊或是惡意軟體透過離埠電子郵件來傳送。

第 2 階段防護方案整合了多重內容控管機制，例如：

- **掃描離埠**與入埠流量中的病毒、垃圾郵件與網路釣魚攻擊
- 透過**內容過濾**來防止敏感、機密或是不當的內容外流，並阻絕詐騙、智慧財產遭竊與意外洩漏機密資訊的風險
- **特徵式的垃圾郵件防護**機制，加上定期的特徵更新，可提供您即時的防護，就算是新興威脅也用擔心

專業的第 3 階段解決方案包括：

- 以軟體、硬體裝置或全新的虛擬硬體裝置形式提供的開道垃圾郵件過濾機制，除了可提供您更高效率的防護能力之外，還能免除網路及用戶端的處理負擔
- 可防護 SharePoint 與其他內容管理系統之類的專業伺服器
- 針對大型的電子郵件環境，或當環境亟需滿足法令或法院要求的電子搜尋規定時，提供歸檔與復原管理工具

備份與復原

許多中小企業都忽略了備份與復原流程，甚至將其視為煩人的問題。不過，受訪企業當中，有半數都曾遺失過諸如財務、法律或是人員記錄之類的重要商業資料、服務層級協議以及代替第三方保管的資訊。以上資料遺失的後果會導致 1/3 的企業喪失商機。而在 25% 從不執行任何備份作業的中小企業，以及超過 50% 將備份檔案與想要保護的電腦存放在同一地點的中小企業當中，就會存在上述漏洞。

使用第 0 階段解決方案的備份作業 (例如複製到 USB 隨身碟或可攜式媒體)，特別是在緊急專案期間，其資料遺失的風險與成本都是最高的。此外，檔案備份無法防止系統當機造成的風險，或是確保所有伺服器與工作站都獲得妥善備份。

第 1 階段的單一功能解決方案則是一大進展。當中最好的部分是可將備份副本移至集中管理的網路儲存位置或安全的線上儲存位置，而其他相輔相成的單一功能解決方案則負責提供系統備份與復原，甚至是集中化管理機制。但這種方式還是存在著很大的缺點，亦即及時且有效的系統復原能力仍嫌不足。

第 2 階段套裝軟體中的資料與系統防護能夠透過以下各項功能來滿足各種管理需求：

- 背景作業能夠在您工作時建立完整的系統備份，完全不會中斷您的生產力
- 集中化監控功能可顯示網路上每一台電腦系統的備份狀態
- 應用程式防護機制可保護重要的 Microsoft® 郵件、內容管理與其他解決方案
- 完整的系統復原能力，包括對虛擬環境的保護

第 3 階段的解決方案可滿足伺服器、遠端辦公室與資料庫等特殊備份需求，包括：

- 滿足特定產業規定與標準架構的特殊需求
- 透過伺服器解決方案來保護儲存在網路、資料庫與其他重要伺服器上的資訊
- 透過特殊設計的功能來符合個別公司在商業模式上的獨特需求

Symantec Protection Suite

賽門鐵克在超過 25 年的歷史中，隨時都在努力協助客戶保護、備份與復原重要的企業資訊，本公司除了細心觀察中小企業的各種防護需求，更透過賽門鐵克全球智慧型網路機制來監控客戶所面臨的各種威脅，然後依據下列原則將豐富的經驗與研究成果整合到適合中小企業客戶的解決方案套裝軟體當中：

- **完整的防護**—多層式防護可突破防毒與基本的備份需求，全方位滿足今日複雜的企業需求。
- **輕鬆的管理**—簡化的技術可讓您快速部署、完美搭配並輕鬆地達到防護目的
- **隨時充滿信心**—清楚、自動化的流程與完整、穩健的桌上型電腦和筆記型電腦復原支援能力，可提供企業不間斷的運作效率，讓企業完全避免緊急事件，或是藉由縝密的計畫及最佳的工具充滿信心地應變

Symantec™ Protection Suite 是第 2 階段的進階解決方案，能夠滿足中小企業最急迫的端點、郵件與備份防護需求。此方案特別針對 5-99 人的小型企業、100-499 人的中型企業分別提供不同的版本，並結合了其他各種產品所沒有的進階功能。這些功能包括：

- 在獨立的防毒有效性測試方面，擁有業界記錄保持最久的完美效能表現
- 電子郵件與即時通訊內容的政策式過濾功能
- 快速復原重要檔案或資料夾以及完整的系統，甚至復原到不同的硬體或虛擬系統都不是問題
- 協調運作不同的技術並提供一致的管理介面，讓您擁有最先進的管理能力

Symantec Protection Suite 將透過賽門鐵克解決方案合作夥伴銷售及支援，這些在安全性與資料防護領域學有專精的合作夥伴遍佈全球，能夠以豐富的知識、經驗與資源適時地為您提供所需的解決方案。這群專家對於中小企業技術與業務需求擁有深入的瞭解，能夠針對本地合作夥伴所設定、建置與管理的第 3 階段進階解決方案提供堅若磐石的基礎。

關於賽門鐵克

賽門鐵克是基礎架構軟體的全球領導者，讓企業與消費者在連線的世界中充滿信心。本公司藉由提供解決安全性、可用性、遵循規範與效能方面風險的軟體與服務，協助客戶保護其基礎架構、資訊與互連性。賽門鐵克總部位於美國加州 Cupertino 市，並在全球 40 個以上的國家地區設有營運據點。如需更多詳細資訊，請上網查詢：

www.symantec.com。

若您需要任何一個分公司的連絡電話或相關資訊，請造訪我們的網站。

台灣賽門鐵克股份有限公司

地址：台北市 105 南京東路 5 段 188 號 2F-7

電話：(02) 8761-5800

傳真：(02) 2742-2838

www.symantec.com.tw