保安資訊有限公司 408 台中市南屯區三和街 150 號 1 樓
http://www.savetime.com.tw/ 電話：886-4-23815000 傳真：886-4-23813000

Symantec™ Messaging Gateway 10.5

功能強大的郵件/訊息安全閘道

型錄：訊息安全

概觀

Symantec™ Messaging Gateway 可提供入埠與離埠的郵件安全以及生產力基礎架構的保護，具備有效且準確的即時防垃圾郵件與防毒保護、目標式針對性攻擊防護、進階內容過濾、防止資料外洩，以及選購的電子郵件加密。Messaging Gateway 易於管理(每5-10分鐘自動更新規則)，可捕獲超過99% 的垃圾郵件，誤報率低於百萬分之一。採用 Messaging Gateway 防禦電子郵件的周邊，企業就能對全新的訊息威脅做出有效的回應、將網路中斷的情況減至最少、維持員工生產力並保護公司的聲譽。

Messaging Gateway 運用來自賽門鐵克全球智慧型網路的即時自動防垃圾郵件與防毒更新，利用全域和自我學習式區域 IP 信譽的內建連線調節功能，以及全方位的報表，讓系統管理員專注於企業的整體安全態勢，同時又能對重要高階主管和管理階層提出有效的報告狀態。進階的內容過濾、防止資料外洩和電子郵件加密則可協助企業控制機密資料，減少與資料外洩有關的風險與成本，同時又能符合法規與企業治理的需求。Messaging Gateway 提供了實體硬體裝置和通過VMware® 認證以及支援 Microsoft Hyper-V 虛擬環境的虛擬硬體裝置，讓企業得以輕鬆地增加功能，在面臨不斷成長的垃圾郵件量時，維持訊息的流通。

降低風險

具備更卓越的效果與個人化威脅偵測的最佳防護

Messaging Gateway 以 Brightmail 防垃圾郵件過濾引擎為後盾 — 這組技術可同時根據全域和區域層級的信譽評等資料來識別電子郵件型威脅。它能讓該軟體將 90% 不請自來的電子郵件到達您的網路之前就加以封鎖，攔截超過 99% 的垃圾郵件，誤報率低於百萬分之一。在獲得全球最大的惡意程式研究組織 — 賽門鐵克全球智慧型網路(Symantec Global Intelligence Network)的支持下，賽門鐵克的訊息安全解決方案結合了來自 1 億 2 千台個裝置和超過 7 千 5 百萬個使用者的即時情報，在不疑有他的受害者與企業受到嚴重破壞之前判別最新威脅。

全球智慧型網路的關鍵在於獲得專利的探測網路 (Probe Network)，這是一個擁有超過 500萬個誘捕電子郵件帳號的系統，主要著重在收集詐騙、網路釣魚和垃圾郵件的樣本。探測網路的範圍遍及全球，包括針對外語內容的部署環境，而且可以評量全球垃圾郵件與網路釣魚活動。這個網路每天收集超過 3 千萬則探測訊息。而賽門鐵克也在更大的規模上每天收集來自匿名客戶的三十億封電子郵件的統計資料，並保護 8 億 5 千萬個以上的信箱，使其免於遭受垃圾郵件和病毒的威脅。SMG 10.5版新增擴充的以 URL 信譽為基礎的過濾會攔截更多垃圾郵件、惡意軟體及網路釣魚訊息。此版本比上一版本的 Symantec Messaging Gateway 包含的威脅 URL 多 70%。URL 被識別為由於目標網站內容的後端分析而造成的威脅。

MG 10.5 版新增「解除威脅(Disarm)」功能:是賽門鐵克全新的技術，可用來防禦目標式攻擊與零時差惡

意程式，方法是將可被惡意程式利用的內容從 Office 和 PDF 附件中移除。它可偵測並移除許多常見電子郵件附件 (包括 Microsoft Office 文件和 Adobe PDF) 中的潛在惡意內容。潛在惡意內容類型包括巨集、程序檔、Flash 影片，以及其他易受攻擊的內容。解除(Disarm)會解構附件、刪除易受攻擊的內容，然後重建文件並保留其視覺逼真度。您可以選擇要「解除」的文件類型和潛在惡意內容類型。您還可以選擇是否封存未經修改的原始文件，以防管理員或一般使用者需要存取它們。

客戶特定規則可讓客戶根據他們視為垃圾郵件的電子郵件或潛在的目標性攻擊輕鬆建立過濾規則。這是一種全新的處置方式，能提高針對式垃圾郵件處置的精確度，針對電子報、行銷電子郵件和包含可疑 URL 的電子郵件提供仔細的新處置方式。客戶可以依自己認為哪些才是不必要的電子郵件，設定這些政策。

身為我們的客戶，您可以將訊息提供給賽門鐵克，賽門鐵克會自動評估您提出的訊息，判斷該訊息是否合法。如果這些訊息不合法，則會建立自動規則與過濾工具，然後提供給貴公司來防護全球攻擊，更重要的是，現在，這些攻擊的特性變得愈來愈具有針對性，並且會鎖定貴公司與一般使用者。

利用防止資料外洩與電子郵件加密獲得更高的掌控度

貴公司的機密資訊外洩很可能會導致您的商譽受損、喪失客戶，最終更將減少營收，這是任何一家公司都無法承擔的後果。Messaging Gateway 具備進階內容過濾與防止資料外洩技術，更容易保護和控制機密資料。系統管理員可以輕鬆建立強制遵循法規的有效與彈性政策，並防止資料外洩。Messaging Gateway 硬體裝置整合了Symantec Data Loss Prevention 精密的結構化資料比對技術，該技術能分析您的資料庫中存放的資料（例如客戶和病患記錄、銀行資料、訂單處理、客戶關係管理等，並且針對實際資料建立特有的比對資料 (fingerprints)。

除了內建與 Data Loss Prevention 的整合性之外，Messaging Gateway 可以做為賽門鐵克領導市場的 Data Loss Prevention 產品之強制執行點，讓您監控與保護透過電子郵件溝通的機密資料，確保資料到達它應該到達的目的地。 與SMG 隔離所無縫整合的能力讓DLP的管理者,直接就能指定所要的動作進行處理，例如直接刪除，或者轉寄給管理者。同時在SMG 與DLP 中間的傳輸是採用傳輸層安全(Transport Layer Security-TLS) 加密,能更強化整體資訊安全等級。

對入埠郵件強制執行 TLS 加密: 透過對來自特定網域的入埠郵件強制執行TLS 加密的選項，可使與信任夥伴和寄件者的通訊更加安全。

Messaging Gateway 提供了一種優質的附加元件 — Symantec Content Encryption，您可以選擇以託管式服務部署或在企業內部部署兩種方式。對於偏好託管型電子郵件加密(hosted encryption)的客戶而言，這項服務是使用 TLS 的技術，將您的郵件伺服器與合作夥伴 (或客戶) 的郵件伺服器之間的完整電子郵件連線 (或管道) 進行加密。它會依據清楚定義、全面而完整且自動強制套用的加密政策，讓您定義與管理專為電子郵件交換而打造的安全通訊。

對於偏好在企業內部加密的客戶而言， Messaging Gateway 可以與以PGP® 技術為後盾的 Symantec Gateway Email Encryption 整合。賽門鐵克的 Symantec Gateway Email Encryption 可設定為閘道模式，而且可以作為 Messaging Gateway 的「武裝」。 Messaging Gateway 可根據需求將標示為要加密的訊息傳送給賽門鐵克的 Symantec Gateway Email Encryption。這些訊息就會被自動加密，並根據加密政策所定義

的方式傳送，因此使用者就可以輕鬆地使用這些訊息

電子郵件是當今企業最常用的通訊方式，而且有愈來愈多的公司快速瞭解到因法規要求將私人資訊加密所衍生出來的加密需求。有了 Messaging Gateway 的內容過濾與防止資料外洩功能，再加上賽門鐵克的內容加密，貴公司就可以避免高額罰款與代價昂貴的資料漏洞，讓您公司的成長不會受阻，並且深知這個不斷演變的威脅版圖也無法拖慢您的腳步。

Messaging Gateway 可提供您穩定的訊息安全解決方案與強化的防止資料外洩及單一廠商的加密策略，降低解決方案蔓延的成本，並減少花費在系統管理與製作報表的時間。

以簡易的管理降低成本與複雜性

彈性與選擇

您的 IT 環境是獨一無二的，而且是專為您的業務需求量身訂做。因此，您對於部署訊息安全的偏好與要求也可能與其他公司有很大的不同。Messaging Gateway 提供彈性的部署選項，可調整以符合您的特定需求。除了在實體硬體裝置上部署 Messaging Gateway 外，您還可以選擇將其部署在虛擬硬體裝置上，這也是訊息安全部署環境中成長最快速的部份。Messaging Gateway 提供了通過VMware® 認證以及支援 Microsoft Hyper-V 虛擬環境的虛擬硬體裝置，使其在保護您的虛擬訊息安全基礎架構的安全方面佔有一席之地。

Symantec Messaging Gateway 10.0 開始支援 IPv6 位址來佈建部署的任何主機，架構掃描程式的程序以及報表。

此外，賽門鐵克是訊息安全領域的市場佔有率領導者，確保與您合作的知名品牌所保護的客戶比任何一家廠商都還要多。由於您的 IT 需求與環境會改變，而威脅也會變得更加複雜，您可以確定的是，賽門鐵克將會提供專為貴公司和您的產業完美量身訂做的安全與穩定的解決方案。

統合式系統管理

Messaging Gateway 內含一個強大的控制中心，可統一管理貴公司的訊息基礎架構。系統管理員可以從單一網頁式主控台輕鬆管理多台 Messaging Gateway 硬體裝置備，以查看趨勢、攻擊統計資料與未遵循法規的事件。透過免除多個主控台、不同政策、以及不相容的登入與報表程序帶來的複雜性，Messaging Gateway 就能大幅減少訊息安全基礎架構的整體持有成本 (TCO)。Messaging Gateway 可支援一組完整的報表選項，包括儀表板和主管摘要，能清楚地突顯出系統功效與影響。報表也可協助系統管理員主動找出資料外洩趨勢，協助企業展現遵循法規的能力。管理主控台包含了 50 種以上可依內容或時間自訂的預先設定報表，報表亦可排程自動產生與匯出。透過圖形訊息稽核介面簡化訊息的追蹤，讓系統管理員快速瞭解通過系統的訊息發生什麼狀況。

針對客戶特定垃圾郵件規則提交郵件(submitting messages for customer-specificspam rules)- 您可以根據管理員與一般使用者提交的遺漏垃圾郵件及誤報郵件，取得特別針對您組織自訂的垃圾郵件規則。架構此功能後，管理員及一般使用者就可以將電子郵件當作遺漏的垃圾郵件或誤報提交給賽門鐵克。在數分鐘內，賽門鐵克便會建立自訂規則集。管道包含規則集，規則集之後會套用到每個已架構的掃描程式。

由於市場趨勢的轉變且垃圾郵件變得更具有針對性，Messaging Gateway 可讓系統管理員針對電子報和行銷電子郵件建立政策，自訂他們對於「不請自來的電子郵件」的定義。此外，透過 Symantec Protection Center 也可以管理 Messaging Gateway，這項單一登入的管理主控台可讓貴公司同時管理和報告與您所有安全解決方案有關的事項。

Messaging Gateway 只需要非常少的設定工作，因此有助於輕鬆且快速地進行初次部署。運用強大的全球智慧型網路可即時自動更新垃圾郵件特徵與病毒定義檔，以簡化管理工作，並協助確保您整家公司具有最新威脅偵測的優勢。

主要效益

- Messaging Gateway 可提供企業實質與可量化的優勢。
- 攔截超過 99% 的垃圾郵件，誤報率低於百萬分之一，並且會自動即時更新。
- 提供目標式攻擊,惡意程式以及零時差攻擊的保護。
- 可自訂垃圾郵件規則-您可以根據管理員與一般使用者提交的遺漏垃圾郵件及誤報郵件，取得特別針對您組織自訂的垃圾郵件規則。架構此功能後，管理員及一般使用者就可以將電子郵件當作遺漏的垃圾郵件或誤報提交給賽門鐵克。只要幾分鐘時間，賽門鐵克即可建立自訂規則。管道(conduit)會取得這些規則，隨即套用至每個已架構的掃描程式。
- Symantec Messaging Gateway 10.0 開始支援 IPv6 位址來佈建部署的任何主機, 架構掃描程式的程序以及報表。
- 以賽門鐵克獲獎的防毒引擎為後盾所提供的最佳防毒保護 (包括零時差防護)，以及自 1999 年 11 月起超過 40 次以上|榮獲 VB100 大獎的保證，透過免於惡意程式的威脅，協助確保企業維持系統運轉率與使用者生產力。
- 保護敏感的客戶資料和寶貴的機密資訊，能夠在訊息或附件中加以比對，以判別真正屬於公司的資料。
- 保護公司信譽並管理與資料外洩、內部治理以及法規遵循相關的風險。
- 選購的 Symantec Content Encryption 線上更新 (subscription) 將電子郵件加密功能整合至 Messaging Gateway 主控台中，並且運用了強大的內建內容過濾與防止資料外洩政策。
- 內含儀表板、摘要報告和詳細報告，可顯示 Messaging Gateway 的功效和影響，同時還可主動突顯威脅趨勢和可能的遵循問題。
- 藉由免除多個主控台、不同政策以及不相容的記錄與報表所帶來的複雜性，降低系統管理成本，同時展現訊息安全的功效與影響。
- 賽門鐵克全球智慧型網路針對垃圾郵件與病毒防護所提供的即時更新衍生自 8 億 5 千萬個以上的受保護信箱、1 億 2千萬個防毒偵測器、以及獲得專利的探測網路中超過 5 百萬個帳戶。
- 在最新和即將出現的威脅造成破壞之前，提供有效、即時的防護。
- 強大、經濟有效且容易使用的 Symantec Messaging Gateway 8300 系列硬體裝置可簡化小型企業的部署工作，並且可擴充至要求最嚴苛的大型企業環境。
- 彈性、可設定、且易於使用的 Messaging Gateway 虛擬版本可在客戶選擇的硬體環境中的 VMware 虛擬機器管理員(Hypervisor) 上執行。

系統需求

支援的平台

Messaging Gateway 可以部署在一系列的 Symantec 8300 硬體裝置上，其擴充性可滿足從小型企業到大型企業的各種環境。此外，我們也提供了虛擬硬體裝置選項，Messaging Gateway 虛擬版本可部署在 VMware 以及Microsoft Hyper-V環境上，提供了相同的軟體、特色與功能。此外，該硬體裝置也可當作專用的控制中心、掃描器或結合控制中心/掃描器部署。

硬體裝置機型	8340	8360	8380
企業規模	中小企業(至1,000位使用者)	企業/大型企業	企業/大型企業
典型部屬	控制中心/掃描器	專用的掃描器或控制中心	專用的掃描器或控制中心
機身大小	1RU高機架型	1RU高機架型	2RU高機架型
電源供應器	一台	備暖、熱抽換式、自動切換、通用電源供應器	備暖、熱抽換式、自動切換、通用電源供應器
處理器	一個多核心處理器	兩個多核心處理器	兩個多核心處理器
硬碟機/RAID	2顆500GB Serial ATA RAID 1	2顆300GB Serial-Attach SCSI (熱抽換式) RAID 1	6顆300 GB Serial-Attach SCSI (熱抽換式) RAID 10
網路介面	2個 Gigabit 乙太網路連接埠	4個 Gigabit 乙太網路連接埠	4個 Gigabit 乙太網路連接埠
*客戶可將任何機型的硬體裝置作為結合控制中心/掃描器、專用掃描器或專用控制中心等形式部署。			

支援的平台

- Symantec Messaging Gateway 8300 系列硬體裝置
- Symantec 8300 系列硬體裝置
- Symantec Brightmail® 8300系列硬體裝置
- Symantec™ Mail Security 8300 系列

虛擬機器管理員（虛擬版本）

- VMware® ESXi/ESX/vSphere 4.x、5.x
- Microsoft Hyper-V 2008或 2012

瀏覽器需求（系統管理主控台）

- Windows® Internet Explorer® 8.0、9.0 或 10.0
- Mozilla® Firefox® 20 或更新
- Google ® Chrome 28 或更新

更多資訊

請造訪我們的網站

http://www.symantec.com/business/brightmail-gateway

與美國的產品專家交談

撥打免付費電話 1 (800) 745 6054

與美國以外地區的產品專家交談

如需特定國家的分公司資訊及聯絡號碼，請造訪我們的網站。

關於賽門鐵克

賽門鐵克是提供安全性、儲存及系統管理解決方案的全球領導廠商，可協助消費者和組織保護及管理其資訊驅動的世界。我們的軟體與服務能夠以更完整、更有效率的方式，在更多的端點避免更多的風險，無論資訊使用與存放的地點為何，都能讓您充滿信心。