Symantec™ Email Security.cloud

服務說明

2018 年 9 月

本服務說明描述了 Symantec Email Security.cloud (以下稱「服務」)。本說明中所有以引號註明之名詞，其定義均為本協議 (定義如下) 或「定義」一節中所解釋之意義。

本服務說明 (隨附參考所包含的任何附件) 是客戶與賽門鐵克之間透過手動或數位方式簽署之協議的一部分並已納入該協議中，用於約束本服務使用，如果此類簽署的協議不存在，則為**賽門鐵克線上服務條款與條件** (以下稱為「協議」)。

目錄

Symantec™ Email Security.cloud

服務說明

2018 年 9 月

1：技術/商業功能及能力

服務概述

Symantec™ Email Security.cloud 是一種託管服務，可過濾電子郵件訊息並協助保護企業不受惡意軟體 (包括目標式攻擊和網路釣魚)、垃圾郵件及大量垃圾電子郵件的侵害。該服務提供了加密及資料保護選項，可協助控制經由電子郵件傳送的敏感性資訊。該服務支援多家廠商的多種信箱類型。

服務功能

- 客戶管理員可以使用受安全密碼保護的登入方式來存取服務管理主控台。管理主控台能讓客戶架構及管理服務、存取報告，以及檢視資料和統計資料 (當服務中有提供這項功能時)。
- 本服務每週七 (7) 天、每天二十四 (24) 小時進行管理，並監控硬體可用性、服務容量和網路資源使用情況。本服務會定期監控其遵循服務等級的情況，並視需要進行調整。
- 服務報告可以透過管理主控台提供。報告可包含活動記錄檔及 (或) 統計資料。客戶可使用管理主控台選擇產生報告，並可設定按照排程以電子郵件傳送，或是從管理主控台下載。
- 服務旨在讓客戶建置有效且可執行的電腦使用政策或同等政策。
- 賽門鐵克提供的建議字詞清單和範本規則或政策包含可能會被視為無禮的字詞。
- 倘若服務因任何原因而暫停或終止，賽門鐵克可能會回復本服務佈建時所做的所有組態變更，而且客戶應該在本服務恢復時負責承擔其他所有必要的組態變更。

服務選項與功能

服務提供兩 (2) 種選項：Email Protect 或 Email Safeguard。選取之選項或附加程式的每位使用者均須購買本服務 (受本服務說明中所述之限制規範)。

各服務選項的功能

	Email Protect	Email Safeguard
電子郵件防惡意軟體：惡意軟體防護，包括網路釣魚及目標式攻擊防護	✓	✓
電子郵件防垃圾郵件：垃圾郵件和網路釣魚 (具備即時連結追蹤功能)，以及大量郵件防護	✓	✓
Email Data Protection：可自訂的內容過濾政策控制		✓
電子郵件影像控制：不當影像偵測		✓
離埠過濾	✓	✓
強制 TLS 加密		✓
隨機 TLS 加密	✓	✓

地址註冊：無效收件者處理	✓	✓
使用者及群組 LDAP 同步工具	✓	✓
郵件追蹤	✓	✓
報告儀表板	✓	✓
摘要 (PDF) 及詳細 (CSV) 報告	✓	✓
一般使用者垃圾郵件隔離所入口網站及通知	✓	✓
免責聲明管理	✓	✓
基礎政策式加密		✓
電子郵件模擬控制		✓

各服務功能的其他資訊可在線上說明中取得，網址為：http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=ZH_TW。

服務附加程式

	Email Protect	Email Safeguard
Advanced Threat Protection: Email	可以使用	可以使用
進階政策式加密	–	可以使用
Email Fraud Protection	可以使用	可以使用
Email Threat Isolation	可以使用	可以使用

各服務附加程式的其他資訊可在線上說明中取得，網址為：http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=ZH_TW。您可在以下網址中找到 Email Fraud Protection 的服務說明：https://www.symantec.com/about/legal/repository。

Advanced Threat Protection: Email 可使用 Symantec Cynic™ 沙箱偵測透過電子郵件傳送的進階威脅，辨識針對收件企業或使用者發動的目標式電子郵件攻擊，以及利用 Symantec Click-time™ URL Protection 找出會在電子郵件傳送後轉變為具有惡意的 URL。透過 O365 客戶適用之 Cynic™ 沙箱可撤回傳送後被確定為惡意的電子郵件。它可提供詳細的惡意軟體報告，包括 URL 資訊、惡意軟體類別、偵測方法以及檔案雜湊。加入資料摘要 API，可透過經驗證的 URL 啟用惡意軟體報告，無須匯入檔案或經由電子郵件傳送資料。Advanced Threat Protection: Email 還提供對網路釣魚演練服務的存取權，該服務是用於確定人員對此類攻擊易受影響程度的網路釣魚攻擊模擬器。使用網路釣魚演練服務，須遵循位於以下位置的條件與條件：https://www.symantec.com/about/legal/repository。

進階政策式加密提供：(i) 提取式網路提取入口網站；(ii) PGP 及 S/MIME 遞送支援；(iii) 嘗試 TLS 加密無效之後，再使用較不透明加密技術的能力；以及 (iv) 加密 .pdf 推送遞送 (Email Safeguard 計劃的基礎政策式加密功能中唯一的加密方法)。進階政策式加密可依據傳送使用者逐一授權，也可以是 Email Safeguard 選項整體使用者數量的一部分。如果客戶需要使用進階政策式加密選項進行安全聲明的傳送，賽門鐵克會讓客戶依據賽門鐵克所定義的公式，按照欲傳送的聲明數量購買額外的使用者授權。

Symantec™ Email Fraud Protection 是一項雲端服務，可自動強制執行 DMARC (Domain-based Message Authentication, Reporting, and Conformance)。與手動方法相較，Symantec Email Fraud Protection 能使每個 DMARC 強制執行步驟變得更簡單且更順暢。強制執行能減輕入

埠模擬攻擊的風險，因為源自未經驗證來源的所有電子郵件會遭隔離或拒絕。強制執行後，電子郵件收件者或郵件傳輸代理程式知道他們可以信任客戶的網域，進而提高電子郵件可傳送率。

Symantec™ Email Threat Isolation 透過隔離惡意連結並安全地轉譯風險網頁，針對魚叉式網路釣魚、憑證竊取和進階電子郵件攻擊加強防護。Email Threat Isolation 使賽門鐵克能夠針對利用惡意連結的複雜電子郵件威脅提供最強防護，例如，進階魚叉式網路釣魚或憑證竊取攻擊。

Email Threat Isolation 會在使用者與其電子郵件連結之間建立安全的執行環境，以遠端轉譯可疑連結，並且僅向使用者顯示未感染的 Web 內容。因此，賽門鐵克可防止任何包含惡意連結的威脅接近使用者，因為所接收的每個連結都將視為惡意並遠端執行，以遠離使用者及其裝置。Email Threat Isolation 還會在唯讀模式下轉譯網路釣魚網站來阻止憑證網路釣魚攻擊，進而防止使用者輸入企業憑證和其他敏感資訊。

服務等級協議

- 賽門鐵克會針對附件 A 中所指定的服務提供適用服務等級協議 (以下稱「SLA」)。

支援的平台及技術需求

- 以下網站提供了本服務的支援平台和技術需求：http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=ZH_TW。

託管服務軟體元件

- 服務包括管理主控台所提供的軟體服務元件，在支付合理費用後即可存取。

2：客戶責任

賽門鐵克只能在客戶提供必要資訊或執行必要動作時執行服務，否則賽門鐵克的服務效能可能會遭到延遲、損害或阻礙，及/或導致服務等級協議權益的適用性無效，說明如下。

- 設定啟用：客戶必須提供必要的資訊，才能使賽門鐵克開始提供服務。
- 適當的客戶工作人員：客戶必須應賽門鐵克的合理要求，提供可協助賽門鐵克交付服務的充足工作人員。
- 客戶應對其帳戶資訊、密碼或其他登入憑證負責。
- 客戶同意使用合理的方式來保護憑證，並將立即通知賽門鐵克有關任何已知未經授權使用客戶帳戶的情況。
- 續購憑證：若適用，客戶必須在帳戶管理內套用適用訂購授權方式或訂單確認函中提供的續購憑證，才能繼續獲得本服務，或保留服務期間內可用的帳戶資訊與客戶資料。
- 客戶組態與預設設定：若適用的話，客戶必須透過管理主控台架構服務的功能，否則將套用預設設定。在一些情況下，預設設定並不存在，而且要等到客戶選擇某設定之後，才會開始提供服務。服務的組態和使用完全是由客戶控制，因此，賽門鐵克不承擔客戶對服務之任何使用的責任，而且對於因客戶操作服務之結果所產生之任何民事或刑事責任概不負責。

可接受使用政策

- 客戶應負責遵守**賽門鐵克線上服務可接受使用政策**。

3：權益與訂購授權資訊

收費規格

本服務依訂單確認函中所指定的以下計量取得：

- 「**使用者**」是指經授權使用服務及/或從使用服務中受益，或實際使用服務任何部分的個人及/或裝置。

訂購授權變更

如果客戶已直接獲得賽門鐵克提供的客戶訂購授權或權益，必須將已允許之客戶訂購授權或權益變更相關通訊內容，傳送至以下地址 (或賽門鐵克公佈的替代地址)：CLD_cancellations_MLABS@symantec.com，除非客戶與賽門鐵克簽訂的協議中另有規定。任何根據此程序發出的通知在收到時即視為已經發出。若客戶經由賽門鐵克經銷商獲得客戶訂購授權或權益，請聯絡客戶的經銷商。

4：協助及技術支援

注意：僅當客戶有權接收賽門鐵克直接提供的客戶協助和支援 (以下稱「支援」) 時，本章節才適用。若客戶有權獲得賽門鐵克經銷商提供的協助和支援，請參閱與該經銷商所簽訂的客戶協議，以取得有關這類支援的詳細資料，此處所述的支援將不適用於客戶。

客戶協助

作為本服務的一部分，賽門鐵克將在當地上班時間提供下列協助：

- 接收及處理服務建置的訂單；
- 接收及處理允許修改服務功能的要求；以及
- 回應帳單及發票的問題。

技術支援

入門級支援將包含作為本服務的一部分，如下指定。

- 每週七 (7) 天、每天二十四 (24) 小時提供支援，協助客戶架構服務功能，以及解決提報的服務問題。我們將會根據發布於 https://support.symantec.com/en_US/article.TECH236428.html 的條款與條件和技術支援政策提供服務支援。
- 指派客戶提交支援問題的嚴重性等級後，賽門鐵克將根據下表中定義的回應目標竭盡全力回應。由於客戶動作所產生之錯誤或需要其他服務供應商採取行動之錯誤，均超出賽門鐵克之控制範圍，因此明確排除在本支援承諾的範圍之外。

問題嚴重性	支援 (全年無休) 回應目標*
一級嚴重性：發生問題，且在下列其中一種情況下無立即可用的因應措施：(i) 客戶的生產伺服器或其他營運關鍵系統已停機或有重大的服務損失；或 (ii) 客戶營運關鍵資料的極大部分處於損失或損毀的顯著風險。	30 分鐘內
二級嚴重性：發生主要功能受到嚴重影響的問題。客戶的營運可在受到限制的情況下繼續，但是長期生產力可能受到嚴重影響。	2 小時內
三級嚴重性：發生問題，但對於客戶業務運作的不良影響有限。	下一營業日的相同時間前**
四級嚴重性：發生問題，且客戶業務運作沒有受到不良影響。	下一營業日內；賽門鐵克會進一步建議客戶將有關新功能或增強功能的客戶意見提交到賽門鐵克的論壇

上述支援回應目標在正常服務運作期間是可以實現的，但是在服務和/或支援基礎架構維護期間不適用，如下方的「維護」一節中所述。

** 目標回應時間與回應要求的時間有關，而不是與解決時間 (解決要求所需的時間) 有關。*

***「營業日」是指客戶當地時區的標準當地上班時間和天數，不包括週末和當地國定假日。在大多數情況下，「營業日」是指客戶當地時區的上午 9:00 至下午 5:00。*

服務和/或支援服務基礎架構維護

賽門鐵克必須不定時執行維護作業。賽門鐵克會善盡商業道義，選擇在總客戶活動度不高的情況下執行例行維護，以盡量減少中斷情形。客戶不會在這些例行維護活動之前收到通知。對於所有其他類型的維護以及如下列所示的維護，賽門鐵克會嘗試在 Symantec Status 頁面上公布警示 (https://status.symantec.com/)，以事先通知受影響的各方。如需服務狀態、計劃性維護和已知問題的相關資訊，請造訪 Symantec Status 頁面並訂閱 Symantec Email Security.cloud 頁面以接收最新消息。**核心服務功能 (例如安全性掃描和電子郵件傳送) 會在所有維護活動期間保持不中斷。**

- ***計劃性維護：***「計劃性維護」是指已排程維護期間，服務在這段期間會因服務基礎架構無法使用而中斷或停止。賽門鐵克會嘗試選擇在客戶總活動度不高的情況下、在受影響基礎架構所在時區內，以及針對網路部分而非全部，執行計劃性維護。進行計劃性維護期間，服務會轉移到未進行維護工作的基礎架構區段，這樣可能不會致使服務中斷。對於計劃性維護，賽門鐵克會善盡商業道義，提前七 (7) 個日曆日在 Symantec Status 頁面上公布以通知客戶。透過訂閱 Symantec Status 頁面，客戶還可透過簡訊、電子郵件或 Twitter 接收通知。
- ***非計劃性維護：***「非計劃性維護」是指已排程維護期間，該期間無法提供標準的七 (7) 天通知，服務在這段期間會因無法提供服務基礎架構而中斷或停止。賽門鐵克會善盡商業道義，至少提前一 (1) 個日曆日在 Symantec Status 頁面上公布以通知客戶。進行非計劃性維護期間，服務會轉移到未進行維護工作的基礎架構區段，這樣可能不會致使服務中斷。有時，賽門鐵克會執行緊急維護。緊急維護定義為必須儘快實作以解決或防止主要資安事端的維護。賽門鐵克會嘗試盡量在維護開始前至少一 (1) 個小時，在 Symantec Status 頁面上公布警示，以提前通知受影響的各方。
- ***管理主控台維護：***對於管理主控台維護，賽門鐵克會善盡商業道義，提前十四 (14) 個日曆日在 Symantec Status 頁面上公布以通知客戶。賽門鐵克會嘗試選擇在總客戶活動度不高的情況下執行管理主控台的維護，以盡量減少管理主控台可用性的中斷。有時，賽門鐵克可能對管理主控台執行輕微更新，客戶不會在這些例行維護活動之前收到通知。

5：其他條款

- 服務是否可全球存取與使用，取決於根據當下賽門鐵克標準的適用出口規範限制與技術限制。
- 賽門鐵克保留修改和更新功能以及服務功能的權利，旨在提供相等或進階服務 (只要賽門鐵克實質上未降低服務核心功能)。客戶確認並同意賽門鐵克保留在訂購授權期間隨時更新本服務說明的權利，以準確地反映所提供的服務，並且更新後的服務說明將在公佈後立即生效。
- 以軟體形式使用任何服務元件時，須遵循軟體隨附之授權許可協議。若服務元件並未隨附使用者授權許可協議 (EULA)，則受到下列條款與條件的規範，網址為：http://www.symantec.com/content/en/us/enterprise/eulas/b-hosted-service-component-eula-eng.pdf。任何與使用此類服務元件有關之其他權利與義務都規定於本服務說明中。
- 除非本服務說明另外指明，否則服務 (及其隨附的任何託管服務軟體元件) 可使用受個別授權約束之開放原始碼及其他第三方資料。
- 賽門鐵克可隨時更新服務，以維護服務的成效。
- 賽門鐵克提供的任何範本僅做為讓客戶可自行建立自訂政策及其他範本的指南使用。
- 服務受到下列限制：
    - 每行事曆月份每位使用者的入埠及離埠郵件數 = 一萬 (10,000) 封。以客戶為目標的垃圾郵件及惡意軟體不在此限制之列。
    - 如果客戶在服務合約上傳明的剩餘月份期間使用量超過了郵件限制，賽門鐵克保留通知客戶並針對超出使用者向客戶收取費用的權利。
    - 入埠與離埠郵件重試排程 = 七 (7) 個日曆日。
    - 預設電子郵件大小上限 = 五十 MB (50MB)。客戶可指定任何電子郵件大小上限，最高為一千 MB (1000MB)。服務接收的任何電子郵件若超過指定限制即會予以攔截及刪除，並會傳送通知警示電子郵件給寄件者、原先的收件者及管理員。
    - 郵件追蹤 = 資料可供疑難排解搜尋達 30 天；單一搜尋可傳回的結果數量另有限制。
    - 惡意軟體隔離所 = 電子郵件會在三十 (30) 天後自動刪除。
    - 垃圾郵件隔離所 = 電子郵件會在十四 (14) 天後自動刪除，除非另有規定。
    - 儀表板報告資料可用性 = 四十 (40) 天 (針對詳細資訊)；十二 (12) 個月 (針對摘要資訊)。
    - 摘要 (PDF) 報告資料可用性 = 十二 (12) 個月。
    - 詳細 (CSV) 報告資料可用性 = 四十 (40) 天。

- 政策式加密受到下列限制：
  - 每月每位使用者的政策式加密 (Z) 離埠電子郵件數 = 三百 (300) 封。
  - 每月每位使用者的基礎或進階政策式加密離埠電子郵件數 = 四百八十 (480) 封。
  - 傳送給多位收件者時，每一個唯一地址即視為一封安全電子郵件。倘若客戶在任何行事曆月份超過允許的安全電子郵件數量，賽門鐵克有權依據實際使用量向客戶收取費用。
  - 透過政策式加密服務路由傳送之電子郵件的大小上限為五十 MB (50 MB)。
  - 若在政策式加密 (Z) 服務中使用提取式加密，根據預設，電子郵件會在安全提取入口網站中儲存 90 天後失效。
  - 若在政策式加密進階服務中使用提取式加密，依據預設，電子郵件會在安全提取入口網站中儲存 30 天後失效。
  - 可用性及延遲服務等級不適用於此服務。

- 為確保訊息在傳輸期間全程受到保護，賽門鐵克建議客戶設定用於政策式加密的網域，例如強制 TLS 加密所有從服務基礎架構離埠及入埠的訊息。
- 客戶必須使用賽門鐵克提供的路由資訊透過賽門鐵克路由傳送入埠電子郵件，不得將電子郵件路由傳送至特定塔台 (Tower) 或 IP 位址。
- 客戶如要使用本服務，則必須擁有自己的電子郵件網域名稱，且能夠設定該網域名稱的 MX 記錄及/或 DNS。
- 客戶必須接受來自所有指定 IP 範圍的入埠電子郵件，以確保在部分基礎架構無法使用的情況下服務的永續性。
- 客戶必須指定郵件伺服器 IP 位址或主機名稱，才能將入埠電子郵件傳送至其企業。
- 客戶必須確定已佈建需要服務的所有網域 (包括子網域)。對於未佈建的網域，客戶同意服務功能可能無法正確運作，且電子郵件可能無法傳送。客戶同意提供及維護要接收服務之有效電子郵件地址的清單 (「驗證清單」)。客戶須負責在服務可用之前以及整個期間內驗證該驗證清單。如果將電子郵件傳送至驗證清單之外或輸入錯誤的電子郵件地址，則服務會拒絕此電子郵件。客戶同意 SLA 不適用於傳送至無效地址的電子郵件。為避免疑義，使用垃圾郵件隔離所系統的客戶必須維護驗證清單，並啟用地址註冊功能。若客戶無法提供上述驗證清單，且申請停用位址註冊功能，賽門鐵克將逐一審查此類申請，並保留自行決定是否拒絕申請的權利。
- 客戶可能釋放分類為包含惡意軟體或垃圾郵件的電子郵件，或要求賽門鐵克在客戶網域中釋放該類電子郵件。 客戶同意，若依客戶要求釋放該類電子郵件，賽門鐵克概不負責。
- 對於因服務未能識別垃圾郵件，或將電子郵件誤認為惡意軟體或垃圾郵件而造成的任何直接或間接損害或損失，賽門鐵克概不負責。賽門鐵克保留掃描所有離埠電子郵件的權利。
- 自佈建服務時起，由服務掃描的電子郵件即會套用預設免責聲明訊息，客戶可透過管理主控台編輯其中的文字。賽門鐵克保留隨時更新預設免責聲明訊息的權利。
- 客戶在使用服務時應遵守所有適用法律。在某些國家或地區，可能需要徵求當事人同意。服務的架構和使用完全是由客戶控制；因此，賽門鐵克不承擔客戶對服務之任何使用的責任，而且對於因客戶操作服務之結果所產生之任何民事或刑事責任概不負責。
- 倘若為客戶持續佈建服務會危害服務的安全，包括但不限於針對或源自客戶網域的駭客活動嘗試、阻斷服務攻擊、郵件炸彈或其他惡意活動，則客戶同意賽門鐵克可以暫停為客戶提供服務。在上述情況下，賽門鐵克會立即通知客戶，並與客戶合作解決上述問題。在移除安全威脅之後，賽門鐵克即會恢復服務。
- 倘若服務因任何原因而暫停，服務就不會運用在客戶的電子郵件上，且電子郵件不會透過賽門鐵克的基礎架構路由傳送。在服務暫停期間，客戶必須負責重新導向其電子郵件，並且確認所有組態在服務恢復時全部正確。
- 倘若服務因任何原因而終止，客戶帳戶將遭到刪除，且客戶將無法存取服務。
- 客戶不得允許其系統：(i) 充當開放式轉送或開放式代理；或 (ii) 傳送垃圾郵件。賽門鐵克保留隨時審查客戶是否遵循本節條款的權利。為避免疑義，凡違反本條款的任何作為即構成重大違反許可協議的情況，賽門鐵克有權立即暫停所有或部分服務，直到違反情況予以改正為止，亦或有權終止與受影響服務相關的許可協議。
- 若在任何時候 (i) 客戶的電子郵件系統被加入黑名單中，或 (ii) 因客戶傳送垃圾郵件，而造成賽門鐵克系統被加入黑名單中，或 (iii) 客戶未能履行本服務說明中所載的任一義務，賽門鐵克將通知客戶，並保留自行決定是否立即暫緩佈建、暫停或終止所有或部分服務的權利。
- 客戶僅允許為自身的商業目的使用服務。客戶同意不轉售、再授權、租賃或以其他方式將服務及相關文件提供給任何第三方使用。客戶同意，未經賽門鐵克事先書面同意，不得將服務用於建置競爭產品或服務，不得以公開發表為目的而複製服務功能或使用者介面、執行服務評估、效能評析或其他比較分析。

6：定義

「**地址註冊**」為服務的強制功能，會拒絕要傳送至不包含在客戶的有效電子郵件地址清單 (「驗證清單」) 中之電子郵件地址的入埠電子郵件。

「管理員」是指經授權代表客戶管理服務的客戶使用者。管理員也許能夠管理客戶指定的所有或部分服務。

「**防垃圾郵件最佳實務設定**」是指賽門鐵克建議的服務組態指導原則，該指導原則會在客戶佈建期間提供給客戶，或公佈在線上說明資源中。

「**連線管理員**」是指 SMTP 交握階段的偵測方法。

「**退款申請**」是指客戶必須以電子郵件提交給賽門鐵克的通知，該通知傳送至 support.cloud@symantec.com，並在主旨行加註「退款申請」(除非賽門鐵克另有通知)。

「**指定塔台叢集**」表示指定為客戶提供 Email Security Services 的兩 (2) 個或更多塔台。

「**網域層級設定**」是指針對 Email Security Services，在管理主控台內對於特定網域可自訂的網域設定。

「**電子郵件**」是指通過服務的任何入埠或離埠 SMTP 郵件。

「**Email Security Services**」是指 Email Safeguard 及 Email Protect 選項和任何可用的附加服務。

「**電子郵件惡意軟體誤報**」是指將合法的電子郵件誤認為包含惡意軟體。

「**一般使用者授權許可協議 (EULA)**」是指軟體隨附的條款與條件 (定義見下文)。

「**全域設定**」是指套用至服務之所有網域及群組層級的管理主控台內動作。

「**群組層級設定**」是指針對服務的相應功能，在管理主控台內對於特定群組的可自訂群組設定。

「**基礎架構**」是指用於提供服務的任何賽門鐵克或授權方技術及智慧財產。

「**已知惡意軟體**」是指在賽門鐵克接收內容之際，已至少提前一 (1) 小時有特徵供賽門鐵克部署之防毒技術使用的惡意軟體。

「**惡意軟體**」是指用於干擾電腦或行動作業，或在沒有適當授權的情況下用於收集敏感資訊及/或取得私人電腦系統存取權的任何軟體。

「**惡意軟體誤報**」是指將合法的電子郵件誤認為包含惡意軟體。

「**成員**」是指利用舊版電子郵件邊界加密附加服務建立加密網路的客戶及其所合作的第三方。

「**月費**」是指協議中所定義之受影響服務的月費。

「**線上說明**」是指 http://help.symantec.com/home/EMAIL_WEB.CLOUD?locale=ZH_TW 中提供的其他資訊。

「**開放式代理**」是指經過架構允許不明或未經授權的第三方存取、儲存或轉送服務的 DNS、網頁或其他資料的代理伺服器。

「**開放式轉送**」是指經架構用於接收來自不明或未經授權之第三方的電子郵件，並將電子郵件轉送至一或多位收件者 (而這些收件者並非是該電子郵件伺服器連線之電子郵件系統的使用者) 的電子郵件伺服器。開放式轉送也可稱為「垃圾郵件轉送」或「公開轉送」。

「**訂單確認**」是指在適用的情況下，「賽門鐵克線上服務條款與條件」中所述的意思。如果服務無適用之條款與條件，則「訂單確認」即為此處定義之訂閱方式。

「**服務**」是指客戶購買的 Symantec Email Security.cloud 的 Protect 或 Safeguard 選項。

「**服務元件**」是指賽門鐵克可分別提供做為服務附屬部分的某些賦予功能之軟體、硬體周邊及相關文件。

「**服務退款**」是指在提交退款申請且經賽門鐵克判定客戶可獲得退款之後，記入客戶下次發票中的金額。

「**服務軟體**」是指軟體 (定義見下文)，可能是服務所需要的，必須安裝在每台客戶電腦上，才能接收服務。服務軟體包括可由賽門鐵克另外提供作為服務其中一部分的軟體及相關文件。

「**軟體**」是指每個賽門鐵克或授權方軟體程式，由賽門鐵克以物件程式碼形式授權給客戶，並受隨附之使用者授權許可協議 (EULA) 的約束，包括但不限於此處所列之新版本或更新版。

「**垃圾郵件**」是指未經收件者許可的商業電子郵件。

「**垃圾郵件漏報**」是指服務未將垃圾電子郵件識別為垃圾郵件。

「**垃圾郵件誤報**」是指服務將電子郵件誤認為垃圾郵件。

「**垃圾郵件建議設定**」是指賽門鐵克建議的服務組態指導原則，在佈建期間提供給客戶或公佈在線上說明資源中。

「**訂購授權方式**」是指一種或多種下列適用文件，其中更進一步定義客戶與服務相關的權利和義務：由賽門鐵克核發的賽門鐵克憑證或類似文件，或客戶與賽門鐵克在服務達成之時、之前或之後訂立的書面協議。

「**Symantec Hosted Service 條款**」是指 https://www.symantec.com/about/legal/service-agreements.jsp 所刊載或透過此網址取得的 Symantec Hosted Services 條款。

「**賽門鐵克線上服務條款與條件**」是指 https://www.symantec.com/about/legal/service-agreements.jsp 所刊載或透過此網址取得的線上服務條款與條件。

「**賽門鐵克追蹤程式**」是賽門鐵克提供的一種工具，用於測量服務的服務可用性及延遲。

「**塔台**」是指負載平衡的電子郵件伺服器叢集。

「**使用者**」是指傳送和接收電子郵件，並且受服務的任何部分所保護的個人。

附件 A

服務等級協議

一般條款

- 若賽門鐵克所提供服務未能符合定義的服務等級，客戶有權申請服務退款。若客戶認為有權要求服務退款，則客戶必須於發生疑似未遵循服務等級事情之當月 (行事歷月) 月底起十 (10) 個工作天內提交退款申請。客戶確知相關記錄僅保留有限天數，因此任何於指定時限範圍外所提出之退款申請將被視為無效。
- 若要提交退款申請，請聯絡賽門鐵克技術支援團隊。請瀏覽下列的產品支援登入頁面，以取得詳細的指示：https://support.symantec.com/en_US/email-security-cloud..html。
- 所有退款申請將由賽門鐵克根據本服務等級協議中適用條款進行核證。賽門鐵克可能要求客戶提供其他資訊以驗證退款申請。
- 本服務等級協議不適用於下列情況：(i) 在執行計劃性維護或緊急維護期間；因不可抗力或客戶或第三方之行為或疏忽而導致無法使用的期間；(ii) 在賽門鐵克根據協議條款而暫停服務的任何期間；(iii) 客戶發生違反協議事件 (包括但不限於客戶發票逾期未付款之情況)；(iv) 客戶未根據協議架構服務的情況；或 (v) 在服務試用期內。
- 本服務等級協議所載補償措施應為客戶就本服務等級協議涉及合約、侵權 (包括但不限於疏失) 等行為主張之唯一補償途徑。
- 在任何行事曆月份，在本服務等級協議下的賽門鐵克累計責任上限應為 100% 全額月費或一萬美元/五千英鎊/一萬歐元 ($10,000/£5,000/€10,000) 的退款 (視客戶發票幣別而定)，以金額較低者為準。
- 如果受影響的服務作為服務套組的一部分購買，則服務退款將根據受影響的服務而非整個服務套組來計算。

Email Security Services 的服務等級協議例外情況

本服務等級協議不適用於下列情況：(i) 未通過服務傳送的任何電子郵件 (包括但不限於客戶未採取適當步驟，以確保僅接受來自賽門鐵克基礎架構的入埠電子郵件)；(ii) 或最初傳送至賽門鐵克時，每個 SMTP 階段作業包含 500 位以上收件者的任何入埠或離埠電子郵件；(iii) 針對佈建於指定為大量叢集塔台之任一塔台的任何客戶；或 (iv) 未佈建服務之客戶網域的任何入埠或離埠電子郵件。

服務可用性

根據 RFC5321，服務可用性的服務等級乃是由從客戶 MTA 的連接埠 25 上，建立將 SMTP 階段作業連線至賽門鐵克基礎架構的能力所決定。服務可用性的服務等級不適用於管理入口網站或垃圾郵件隔離所系統。如果客戶錯誤地架構服務，或因無法預期之狀況或超出賽門鐵克可合理控制之事由 (包括但不限於自然災害、戰爭、恐怖主義、暴動、政府行為，或賽門鐵克資料中心外部 (包括位於客戶網站中或位於客戶網站與賽門鐵克資料中心之間) 的網路或裝置故障)，本服務等級則不適用。

若服務可用性在任何行事曆月份均低於百分之百 (100%)，客戶可提交退款申請，並可能收到 100% 全額月費或一萬美元/五千英鎊/一萬歐元 ($10,000/£5,000/€10,000) 的服務退款 (視客戶發票幣別而定)，以金額較低者為準：

每行事曆月份的可用百分比	月費退款百分比
低於 100%，且高於或等於 99%	25%
低於 99%，且高於或等於 98%	50%
低於 98%	100%

若服務可用性在任何行事曆月份均低於百分之九十八 (98%)，且經過賽門鐵克確認，則客戶有權終止受影響的服務，並依據終止生效後的期間部份按比例獲得預付費用的退款。

電子郵件傳送

電子郵件傳送服務等級由賽門鐵克能否百分之百傳送客戶入埠或離埠電子郵件的能力決定，但受下列條件的限制：

a) 賽門鐵克必須收到電子郵件；且

b) 電子郵件不得包含惡意軟體、垃圾郵件或其他會導致服務遭受攔截的內容。

依據前述條款之規定，若賽門鐵克無法向/從客戶傳送電子郵件，且客戶未違反本協議之條款，客戶即有權在三十 (30) 個日曆日之前，以書面通知方式終止服務。

電子郵件延遲

電子郵件延遲服務等級由以下因素決定：客戶指定塔台叢集內各個塔台每隔五 (5) 分鐘接收自另一個塔台寄出的電子郵件的平均來回時間 (由賽門鐵克追蹤程式測定) 是否超過下表所規定的延遲時間 (以行事曆月份計)。若客戶認為延遲服務等級未達標準，可提交退款申請，並可能收到根據下表所規定的服務退款：

平均來回時間 (秒)	月費退款百分比
高於 60，且低於或等於 90	25%
高於 90，且低於或等於 120	50%
高於 120，且低於或等於 180	75%
高於 180	100%

本延遲服務等級不適用於下列情況：

a) 客戶未提供賽門鐵克驗證清單，且客戶遭受阻斷服務攻擊；

b) 延遲時間是因往返客戶系統的郵件循環傳遞所造成；或

c) 客戶的主要電子郵件伺服器在初次嘗試傳送時無法接受電子郵件。

垃圾郵件誤報

垃圾郵件誤報服務等級將定義最高垃圾郵件誤報捕獲率。垃圾郵件誤報服務等級僅適用於以下情況：客戶已建置線上說明資源中所提供的防垃圾郵件最佳實務設定。若垃圾郵件誤報平均捕獲率在任何行事曆月份超過客戶入埠電子郵件流量的 0.0003%，客戶可提交退款申請，並可能收到根據下表所規定的服務退款：

垃圾郵件誤報捕獲率百分比	月費退款百分比
高於 0.0003，且低於或等於 0.003	25%
高於 0.003，且低於或等於 0.03	50%
高於 0.03，且低於或等於 0.3	75%
高於 0.3	100%

基於本服務等級的目的，下列電子郵件不構成垃圾郵件誤報電子郵件：

a) 不屬於合法商業電子郵件的電子郵件；

b) 包含 20 位以上收件者的電子郵件；
c) 電子郵件的寄件者在客戶的攔截寄件者清單上，包括但不限於客戶啟用使用者層級設定時，個別使用者定義的攔截寄件者清單；
d) 由受感染的機器所傳送的電子郵件；
e) 傳送電子郵件的機器在第三方攔截清單上；
f) 由離埠垃圾郵件掃描所攔截的電子郵件。

客戶必須在收到電子郵件的五 (5) 個日曆日內將疑似誤報的電子郵件回報賽門鐵克技術支援團隊，才符合服務退款的資格。賽門鐵克會調查並確認電子郵件是否為垃圾郵件誤報，並記錄調查結果。

垃圾郵件捕獲率

垃圾郵件捕獲率服務等級將定義最低垃圾郵件捕獲率。本服務等級僅適用於以下情況：客戶已實作線上說明資源中所提供的防垃圾郵件最佳實務設定。服務等級對應的是某個行事曆月份中測得的垃圾郵件漏報數量。客戶可提交退款申請，並可能收到根據下表所規定的服務退款：

垃圾郵件捕獲率 %	月費退款百分比
高於 98，且低於或等於 99	25%
高於 97，且低於或等於 98	50%
高於 96，且低於或等於 97	75%
低於 96	100%

本垃圾郵件捕獲率服務等級不適用於以下情況：電子郵件並非傳送至有效的電子郵件地址。包含百分之五十 (50%) 以上雙位元字元集的電子郵件適用百分之九十五 (95%) 的低垃圾郵件捕獲率。倘若上述垃圾郵件捕獲率低於百分之九十五 (95%)，客戶有權要求百分之二十五 (25%) 月費的服務退款。倘若垃圾郵件捕獲率低於百分之九十 (90%)，客戶有權要求百分之百 (100%) 全額月費的服務退款。

客戶必須在收到電子郵件的五 (5) 個日曆日內將疑似漏報的電子郵件回報賽門鐵克技術支援團隊，才符合服務退款的資格。賽門鐵克會調查並確認電子郵件是否為垃圾郵件漏報，並記錄調查結果。

惡意軟體防護

若客戶系統因通過雲端掃描服務的電子郵件而感染已知惡意軟體或不明惡意軟體，則客戶有權要求如下定義的服務退款金額。客戶必須在知曉此類惡意軟體後的五 (5) 天內通知賽門鐵克，且此類通知必須由賽門鐵克記錄、調查和驗證。客戶必須提交退款申請，並在通過驗證後，收到百分之百 (100%) 全額月費或一萬美元/五千英鎊/一萬歐元 ($10,000/£5,000/€10,000) 的服務退款 (視客戶發票貨幣而定)，以金額較低者為準。本節所載補償措施應為就合約、侵權 (包括但不限於疏失) 等行為，或透過服務傳給客戶或第三方惡意軟體而受到感染之情況，所主張之唯一專屬補償途徑。為避免疑義，本節所載補償措施不適用於蓄意自我感染的情況。

若透過服務和惡意軟體接收之電子郵件中所附加的惡意軟體，已經自動或透過手動介入而在客戶系統內啟動，則客戶系統就視為已受感染。若有賽門鐵克偵測但未阻擋帶有惡意軟體附件的電子郵件，並在 Symantec Status 頁面上公佈了更新或通知了客戶，且提供足夠資訊讓客戶可辨識和刪除受感染的電子郵件，則上述補償措施將不適用。

服務會盡最大可能掃描所有電子郵件及其附件。服務可能無法掃描附件內容受寄件者直接控制的附件 (*例如*，受密碼保護及/或加密的附件，及 (或) 與電子郵件分開傳送的密碼)。此類電子郵件及/或附件將排除在服務等級之外，且不適用上述補償措施。

本惡意軟體防護服務等級不適用於由客戶蓄意釋放的惡意軟體，或在客戶的要求下由賽門鐵克蓄意釋放的惡意軟體。

本惡意軟體防護服務等級僅適用於本服務說明中定義的惡意軟體，不適用於下列項目：間諜程式、廣告軟體、裝載惡意內容之網站的 URL 連結，或不明特洛伊木馬程式。

惡意軟體誤報

惡意軟體誤報服務等級將定義最高惡意軟體誤報捕獲率。若電子郵件惡意軟體誤報捕獲率在任何行事曆月份超過客戶電子郵件流量的 0.0001%，客戶可提交退款申請，並可能收到根據下表所規定的服務退款：

惡意軟體誤報捕獲率百分比	月費退款百分比
高於 0.0001，且低於或等於 0.001	25%
高於 0.001，且低於或等於 0.01	50%
高於 0.01，且低於或等於 0.1	75%
高於 0.1	100%

全年無休技術支援與錯誤回應

每週七 (7) 天、每天二十四 (24) 小時提供技術支援以便：

a) 為服務發生問題的客戶提供技術支援；及

b) 與客戶溝通以解決此類問題。