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

# 以 PGP ™ 技術為後盾的 Symantec Endpoint Encryption

## 產品型錄：端點加密

### 保護您的客戶及企業

保護客戶隱私與員工以及財務資料、智慧財產、商業策略、開發計劃等資訊並減輕資料外洩的影響，是推動當今大多數企業部署加密解決方案的主要因素。現在，網路攻擊的技術複雜性與發動頻率均呈指數上升態勢，因此資料外洩事件出現劇增的現象也就不足為奇了。根據 2013 年的賽門鐵克網路安全威脅研究報告，資料外洩比以往高出 62%，而且其中至少有 8 起資安事端暴露了超過 1 千萬筆個人身份。企業也付出更多復原的成本。2013 年，公司受資料外洩影響所付出的平均成本為每次 350 萬美元，每筆 145 美元，相較前一年增加了 15%。2014 年資料外洩事件數量又比前一年增長 23%，而每起事件中洩露的身份資訊平均高達 110 萬筆。企業挽回資料外洩損失的代價也越來越大。但是你的數據不會只有駭客的風險。意外暴露和設備遭竊 / 遺失佔這些違規事件的 56%。

法規要求使得加密成為許多企業的必要課題。若企業必須需要遵守如 PCIDSS 或 HIPAA 之類的法規，則必須擁有可稽核的加密解決方案，才能保護客戶資料的隱私。在許多情況下，發生資料外洩時，企業必須通知受害者及主管部門發生了什麼情況。若有加密解決方案，企業就可適用「安全港」，發生資料外洩時，就不需要對外公開。

法規要求使得加密成為許多企業的必要課題。若企業必須遵守如台灣政府在 2012 年十月一日施行生效的個人資料保護法，美國的醫療保險可攜性與責任法案 (the Health Insurance Portability and Accountability Act of 1996, HIPAA）、經濟與臨床健康資訊科技法（Health Information Technology for Economic and Clinical Health Act；以下簡稱 HITECH）、支付卡產業資料安全標準 (PCI- DSS: Payment Card Industry Data Security Standard) 金融服務業現代化法 (GLBA: Gramm-Leach-Bliley Financial Modernization Act)、沙賓法案」(SOX:Sarbanes-Oxley Act)、 巴塞爾協定（Basel II）、歐盟資料防護指令（ 指令 95/46/EC- EU DPD)、英國資料保護法 (UK Data Protection Act) 以及美國州層級資料外洩通知法律之類的法規，則必須擁有可稽核的加密解決方案，才能保護客戶資料的隱私。在許多情況下，發生資料外洩時，企業必須通知受害者及法規主管單位發生了什麼情況。若有加密解決方案，企業就可適用「安全港」，使業者倘不幸遭遇資料外洩事件，得主張資料已施行適當之加密保護，即無需承擔龐大外洩通知成本之衡平規定。

### 全方位的端點加密

筆記型電腦、隨身碟與抽取式硬碟等端點裝置遺失和遭竊，仍是資料外洩的主要原因

- **最高防護能力 -** 在一開始加密的階段， Symantec Endpoint Encryption 會逐一依磁區將每一台磁碟機加密，確保所有檔案都確實加密，以便獲得最高的防護能力。
- **易於使用** - 加密之後，使用者只需輸入一次密碼，單一登入技術就會引導使用者進入主畫面，不需要重新輸入多組密碼。當使用者存取其資訊時，會立即執行解密及重新加密，以提供流暢的體驗。
- **多種復原選項** - 多種復原選項可讓企業找到最適合使用者的自動復原及技術支援中心組合。本機自動復原能讓使用者設定可自訂的問題與答案，以便重新取得登入權限；而技術支援中心則可提供一次性的權杖 (token)，供使用者插入電腦。這是一項附加的安全措施，此權杖在每次使用後就變更。
- **彈性的抽取式媒體** - 抽取式媒體的使用者可以在任何 Windows 或 Mac 系統上存取其資料，即使所使用的電腦並未安裝加密功能。Symantec Endpoint Encryption 支援各種類型的可移動媒體，包括 USB 隨身碟，外接式硬碟和 CD / DVD / 藍光媒體。

## 企業級管理功能

**建置加密解決方案時，自動化及金鑰管理是成功的關鍵。**Symantec Endpoint Encryption **提供了一套整合式管理平台，讓企業從單一主控台迅速部署及管理其端點加密解決方案**

- **高擴充性 -** 相較於之前的平台，改進的管理架構可提供更卓越的擴充性，並且能輕鬆因應大型企業環境。
- **自動化** - 系統管理員可以運用 Active Directory 同步處理使用者與群組的設定檔，將整個企業內的金鑰管理及政策控管自動化、加速部署，進而減少系統管理負擔。
- **健全的報告 -** 法規遵循報告立即可用，也可以自訂，協助減輕向稽核員及主要業務關係人證明的負擔。
- **異質化加密** - 管理功能已經擴充到包括支援原生作業系統加密 (FileVault2) 與遵循 Opal 規定的自我加密磁碟機。

## 透過 Symantec Data Loss Prevention 提高安全性

**由於使用者的疏失，機密資料經常被傳輸至未受保護的裝置。**Symantec Endpoint Encryption **整合領先業界的** Data Loss Prevention (DLP) **解決方案，可協助解決此問題。**

**由於使用者會在筆記型及桌上型電腦上不斷地累積資訊，因此** DLP **會掃描這些資料、標示出敏感內容，並監控使用者上線及離線的活動。如果使用者試圖將機密資料移至抽取式裝置，**DLP **會記錄動作，而不是光封鎖傳輸，因為這樣可能會阻礙使用者。接著，透過可自訂的提示畫面，員工會獲知自己正嘗試移動敏感檔案。接著，在授權傳輸前，系統會提供使用者先將檔案加密的選項，讓企業主動預防使用者的疏失，並確保業務永續性，同時協助教育員工遵循最佳實務準則。**

## 其他加密選項

**只要有賽門鐵克，您的安全解決方案不只是端點加密。企業可以利用市場上最廣泛的加密產品組合，並運用例如電子郵件、檔案及資料夾加密等解決方案，保護其他通訊管道。**

| | |
|---|---|
| **端點加密： 您如何在保護端點上的機密資料的同時符合各種法規與遵循規定？** | |
| **端點加密** | **以 PGP™ 技術為後盾的 Symantec Endpoint Encryption:**<br>● **它能讓企業針對桌上型電腦、筆記型電腦或抽取式媒體上的資料提供全磁碟加密及管理功能，並且能夠與 Symantec Data Loss Prevention 整合。直覺式的管理介面可協助企業擴充部署環境，並具備立即可用的法規遵循報告以及可自訂報告。管理功能包括針對原生作業系統加密 (FileVault2) 與遵循 Opal 自我加密磁碟機的支援功能。** |
| **電子郵件加密**：由於客戶與公司之間會透過電子郵件傳送大量資訊，您要如何確保無論在公司防火牆的內部或外部，只有經過授權的個人才可以看到這些資訊？ | |
| **閘道電子郵件加密** | **以 PGP™ 技術為後盾的 Symantec Gateway Email Encryption:**<br>● **Symantec Gateway Email Encryption 提供集中管理的電子郵件加密功能，無論收件人是否擁有電子郵件加密軟體，均可保護您和客戶及合作夥伴之間的電子郵件通訊安全。利用 Gateway Email Encryption，企業就可以減少資料洩漏的風險，同時確保遵循資訊安全與隱私權的相關法規。在不影響一般使用者體驗的情況下保護離埠通訊，並且無須使用用戶端軟體。同時為收件者提供無須加密的安全傳遞選項。** |
| **桌面電子郵件加密** | **以 PGP™ 技術為後盾的 Symantec Desktop Email Encryption:**<br>● **提供以用戶端為基礎的電子郵件加密功能，可對桌上型電腦和筆記型電腦上傳送及接收的電子郵件，自動進行加密及解密，以保護端對端通訊的安全。提供端對端的電子郵件加密，可直接在用戶端之間自動對電子郵件進行加密和解密，而不需要登入第三方網站。無論電子郵件在內部郵件伺服器上，或委外至雲端，均可維持加密的狀態。** |
| **檔案及資料夾加密**：協同合作和檔案共用能夠強化員工的效率，但由於檔案數量不斷倍增並且四處移動，您要如何保護您的資料避免意外或惡意的暴露？ | |
| **專為協同合作團隊設計、由政策強制執行的檔案加密檔案共享加密** | **以 PGP™ 技術為後盾的 Symantec File Share Encryption:**<br>● **利用強制執行政策對檔案與資料夾進行加密，實現團隊協同合作及雲端共用的目標。自動且透通地加密檔案伺服器和共用網路磁碟機上的檔案和資料夾，並利用拖曳方式讓您輕鬆共用受保護的檔案及避免資料無計劃地增加。** |

| | |
|---|---|
| 保護自動化業務流程中的機密資料 - 檔案傳輸和資料處理應用程式的加密 | **以 PGP™ 技術為後盾的 Symantec Command Line：**<br>● Symantec Command Line 能讓企業快速且輕鬆地將加密功能整合至批次處理、程序檔和應用程式中，以確保企業資料在儲存或傳輸中的安全性。無論您的挑戰是保護信用卡資訊、金融交易、薪資、醫療記錄或其他機密資訊，Command Line 可撰寫程式化語法的加密功能都是企業資料保護工具組中不可或缺的一部分，讓企業能快速且輕鬆地將加密功能整合至批次處理、程序檔和應用程式中，以確保企業資料在儲存或傳輸中的安全性。 |

## 系統需求：

| | |
|---|---|
| 管理伺服器 (Server) | ● Microsoft Windows Server 2012 R2, 2008 R2<br>更多詳細需求<br>https://support.symantec.com/en_US/article.TECH224478.html |
| 管理主控台 (Console) | ● Microsoft Windows 10,8.1, 8, 7。<br>● Microsoft Windows Server 2012 R2, 2008 R2<br>更多詳細需求<br>https://support.symantec.com/en_US/article.TECH224479.html |
| 用戶端 (Clients) | ● Microsoft Windows 10,8.1, 8, 7。<br>● Microsoft Windows Server 2012 R2, 2008 R2<br>● Mac OS X 10.10.5, 10.10.4<br>更多詳細需求<br>https://support.symantec.com/en_US/article.TECH224480.html |
| 與 Directory 的整合性 | Microsoft® Active Directory |
| 更多詳細需求 | https://support.symantec.com/en_US/article.TECH224902.html |

## 更多資訊 請造訪我們的網站

http://www.SaveTime.com.tw（好記：幫您節省時間.的公司.在台灣）

## 關於保安資訊：

**從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值**

- 保安資訊被業界公認為最專業的賽門鐵克解決方案的專家。
- 保安資訊的團隊自 1995 年起就專注於賽門鐵克資訊安全解決方案的銷售、規劃與整合、技術支援、教育訓練、顧問服務，特別是提供企業 IT 專業人員的技能傳承 (Knowledge Transfer) 的效益上，以及比原廠更快速的技術支援回應，深獲許多中大型企業與組織的青睞（特別是有 IT Team 的組織），長期合作的意願與滿意度極高。
- 與許多系統整合或服務公司不同的是，我們不吝惜分享我們的專業技能與經驗給顧客的 IT Team，經由常態性的教育訓練、精簡的快速手冊以及標準 SOP 文件的提供，以及基於比原廠更孰悉顧客的使用環境與現況的快速回應的品質，在業界建立扎實的口碑。
- 保安資訊一直專注於賽門鐵克領先業界的資訊系統基礎架構上的安全性與可用性的解決方案。進而累積了許多與基礎架構整合的成功經驗，讓導入 Symantec 解決方方案的成效非常卓越。我們的顧客都能免除 Try & Error 的時間浪費及不確定的投入或自行摸索的運作風險。
- 保安資訊聯絡資訊 http://www.savetime.com.tw 0936-285588