

以 PGP™ 技術為後盾的 Symantec Encryption Management Server

產品型錄：加密

管理多種加密解決方案變得愈來愈困難

許多企業戰術性地使用加密技術，在需求產生時採用各種不同的單一功能解決方案。不幸的是，在部署單一功能解決方案來保護硬碟、電子郵件和檔案時，通常也必須部署與管理多種管理主控台。在以及時而合乎成本效益的方式確保正確強制執行政策與部署時，這種零碎的方式會增加複雜性與系統管理工作量。

Encryption Management Server 能管理並自動化所有賽門鐵克加密解決方案的安全政策，以捍衛敏感資料並防止因資料外洩而可能導致的財務損失、違法後果與品牌受損。

降低成本與複雜度



- 統一的系統管理主控台 - 免除維護多個加密主控台的成本，並將安全政策不一致的風險降到最低。
- Symantec Protection Center - 整合多種安全性產品的系統管理與報告功能。
- 記錄、監控與報告 - 減少就多種加密解決方案進行稽核所需的時間。
- 企業整合 - 使用選購的企業目錄整合、PKI 或企業系統管理工具，微調政策的指派。

自動部署與後續管理

Server 會自動化進行賽門鐵克加密解決方案的部署、資源配置、金鑰管理與政策強制執行，降低系統管理員工作量並確保整個企業內擁有一致的安全政策。

系統管理員可從單一網頁式管理主控台，跨多種整合式加密解決方案即時建立、強制執行與更新安全政策。此外，亦可使用選購的企業目錄整合，微調加密政策的指派。

根據明日需求所打造，同時滿足今日的安全需求

Encryption Management Server 能讓企業同時就戰術上與策略上採用加密。系統管理員可運用 Encryption Management Server 的集中化管理功能，隨著企業成長逐步建立其加密架構，同時維持掌控度與秩序。

為了更易於使用，主控台內建了更多的加密功能，讓系統管理員使用簡單的授權來啟用新功能，在需要時輕鬆地新增與部署工具，而無需在用戶端電腦安裝新軟體。

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

PGP™ 技術為後盾的 Symantec Endpoint Encryption:

- 它能让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:

- 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。

<p>桌面電子郵件加密</p>	<p>以 PGP™ 技術為後盾的 Symantec Desktop Email Encryption:</p> <ul style="list-style-type: none"> ● 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。
<p>行動電子郵件加密</p>	<p>由於企業使用者及其裝置越來越行動化，賽門鐵克的加密解決方案可讓使用者從智慧型手機與其他 iOS 裝置 (包括 iPad®) 輕鬆傳送及接收加密的電子郵件。</p> <ul style="list-style-type: none"> ● Mobile Encryption for Apple® iOS 裝置 - 電子郵件加密。 ● PGP Viewer for Android™ 裝置 - 電子郵件加密檢視器。 ● PGP support Package for BlackBerry- 電子郵件加密。 <p>- iOS 和 Android 適用的電子郵件應用程式已經在 Apple App Store 和 Google Play 上架。</p> <p>- 行動解決方案必須使用 Encryption Management server 才可為使用者提供登錄服務以及進行金鑰管理。</p>
<p>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？</p>	
<p>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</p>	<p>以 PGP™ 技術為後盾的 Symantec File Share Encryption:</p> <ul style="list-style-type: none"> ● 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。 ● 在採用雲端做為實際的生產力工具之前，企業必須對於將資料儲存在雲端的安全性深具信心。File Share Encryption 可讓使用者以托放方式將未加密的檔案移至共用資料夾中自動進行加密。在檔案移出後，仍將保持其加密狀態，因此只有獲得授權的使用者得以檢視機密資料。 ● File share encryption for iOS，可在 iOS 裝置上檢視採用檔案共用加密的檔案。
<p>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</p>	<p>以 PGP™ 技術為後盾的 Symantec Command Line:</p> <ul style="list-style-type: none"> ● 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、流程自動化、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。

技術需求

Encryption Management Server

支援的系統管理專用網頁瀏覽器	VMWare vSphere 5.1 VMWare ESXi 5.0 或 6.0
與 Directory 的整合性	Microsoft Active Directory 2008-2012 Lotus Notes/Domino Directory 9.0.1 FP4 OpenLDAP 4.x
如需詳細的硬體規格：	https://support.symantec.com/en_US/article.TECH234481.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，以及基於比原廠更熟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