玉山科技股份有限公司
http://www.asiapeak.com
(02)77128295

善用PGP加密工具的六大技巧

(原載 IThome 企業資安專刊, 2008/4/15 出版)

資料加密的必要性

根據 Forrester Research 研究，過去大家都把資安重點放在 IT 環境(Infrastructure-level)的層層防護上(例如防火牆、入侵偵測、防毒等)，而忽略了資料(Data-level)的防護，未來無論是企業或個人，以資料為中心的(Data Centric)防衛策略會越來越重要。

筆記型電腦遺失或被偷、硬碟被盜、隨身碟遺失、電腦送修時資料被複製出去、磁帶或光碟寄送過程中遺失、電子郵件或 FTP 傳檔中被攔截竊取…等等每日層出不窮的新聞報導，讓大家對電腦既喜愛又怕受傷害。其實只要一些很簡單的方法與工具，就可免除這些資料遺失或外洩的風險。將資料加密起來，讓不相干的人即使拿到也毫無用處，這是資料安全最簡單也是最根本的做法。

加密的方法

所謂資料加密，就是透過某種方法將明文資料亂碼化，讓人看不懂；當本人要使用時再把它解密回來。至於這亂碼過的資料是否容易被破解？這就涉及使用的「亂碼方法」(Cryptography 密碼學)了。一般加密方法分為兩類，一是對稱式加密，使用同一把金鑰(Key)來加密與解密，常見的對稱式演算法如 DES, 3DES, AES 等；另一類是非對稱式演算法，使用一對金鑰(公鑰與私鑰)來加解密，用公鑰加密過資料只有用其對應的私鑰才能解得回來，而用私鑰加密過資料只有用其對應的公鑰才能解得回來；公鑰可以公開出去，私鑰則必須好好保管在自己的電腦裡，常見的非對稱式演算法如 RSA, DSA 等。這兩類加密演算法主要用途不同，在此不再細述。加密的強度(容不容意被破解)還依靠使用金鑰的長度及如何產生及保管金鑰。金鑰如果是隨機產生(Random)而不是人為選擇的，通常只能用「暴力」法來破解，這就要看需要花多少時間與成本了。

如何選擇好的加密工具

一個好的加密工具軟體至少需俱備：

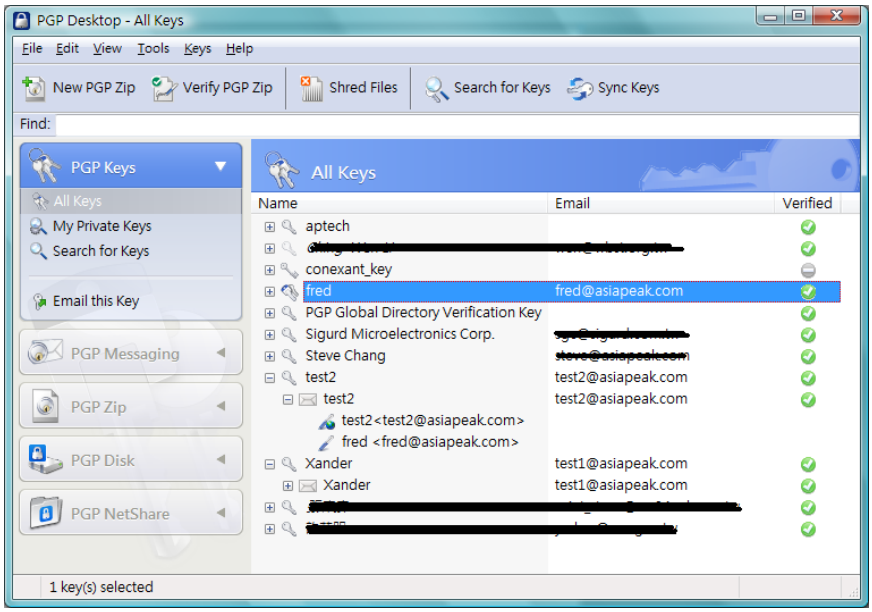
1. 支援最新最安全的主流加密演算法；
2. 支援最大金鑰長度；
3. 容易使用的操作介面及金鑰管理；
4. 經過長時間眾多使用者的粹練；

5. 可以同時用在 email 加密，檔案加密等不同目的。

PGP 加密工具軟體

PGP 加密軟體從早期的免費版本到近年來的商業版本，十多年來已有超過三百萬個使用者，尤其在商務應用上，全球百大企業 80%使用它在內部人員電腦以及外部商業夥伴的機密資料往來。

PGP Desktop 軟體功能眾多，但使用上非常容易。因為 PGP 主要使用非對稱式加密, 所以要先產生一組 Key Pair， 你可以選擇金鑰長度，越長越安全，但相對地加解密越花時間；內定是 2048bit RSA Key，這 key pair 包括一支公鑰及一支私鑰，你也可以產生很多 key pair，可以一個 key pair 對應一個 email 帳戶，或不需要 email 帳戶，如果你想用在其他加密用途，但是太多 key pair 只會混亂自己，除非你記憶力很好。到這裡你已經可以保護自己電腦裡面的資料了，如果你想與別人分享私密資料，你必須與他們交換公鑰。你可以 Export 自己的公鑰寄給你的親朋好友，也可以上傳到 PGP 的公鑰伺服器(PGP Global Directory Key Server)，想要與您「親密」往來的人可以下載您的公鑰。這些動作都是在 PGP 工具畫面下可以完成的。接下來你要將別人的公鑰 Import 進來， PGP 畫面裡的 All Keys 就是讓你管理所有的金鑰；你也可以將 key pair (或私鑰)放在 USB Token 裡，當你要使用私鑰時，必須插入此 Token，並輸入密碼驗證，這樣做更安全。



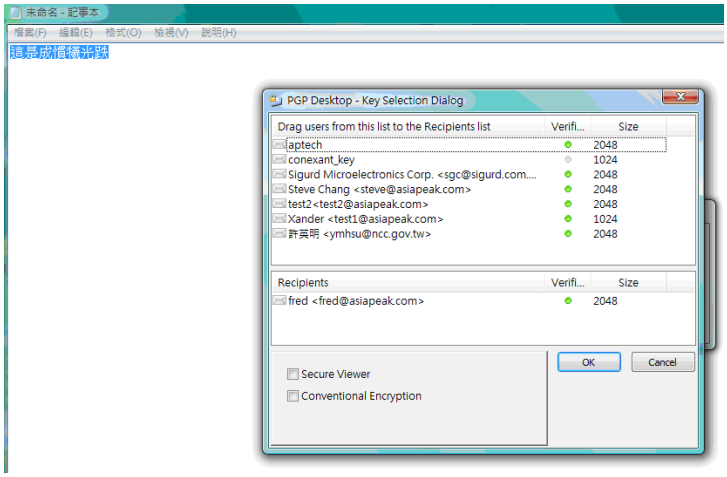
PGP 使用技巧一：電子郵件加密

擔心寄出的電子郵件內容被人看光光? 會不會收到偽冒的電子郵件? PGP 可以自

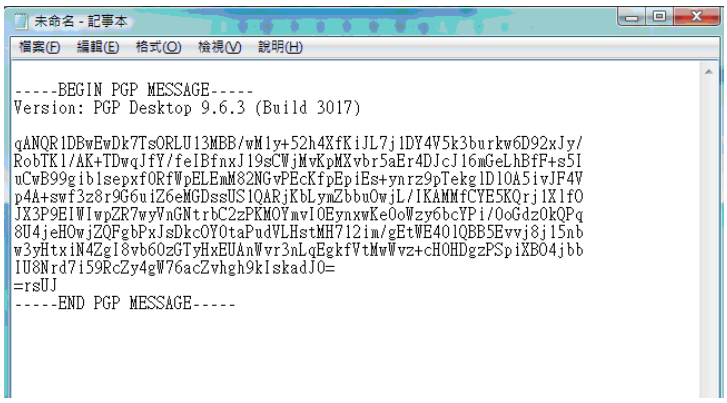
動地幫您做 eMail 加密及簽章。

你可以自己設定各種安全政策，例如收件人是誰、主旨內容為何時就需要加密與簽章，其他情況可以只簽章(證明這信是我本人發的)而不加密；你只要將 PGP Mail Proxy service 打勾，PGP 就依照您設定的政策自動執行，PGP 會找出收件人的公鑰，使用此公鑰來加密郵件內容，再用你自己的私鑰來簽章這郵件；對方 PGP 收到這郵件時，會先用你的公鑰來驗證這郵件確是你寄出的，然後用他自己的私鑰來解開這郵件內容。這所有動作都由 PGP 在背後自動執行。

你也可以不用 PGP Mail Proxy Service，你自己可以先用 Notepad 之類的工具編寫郵件內文，然後按 PGP Icon 選擇 [Current Window]， 再選擇 [Encrypt & Sign] 或 [Encrypt]，就會出現你電腦裡所有公鑰的人讓你選擇，你可以選取多個人，這些人就是可以解密你加密的內容。

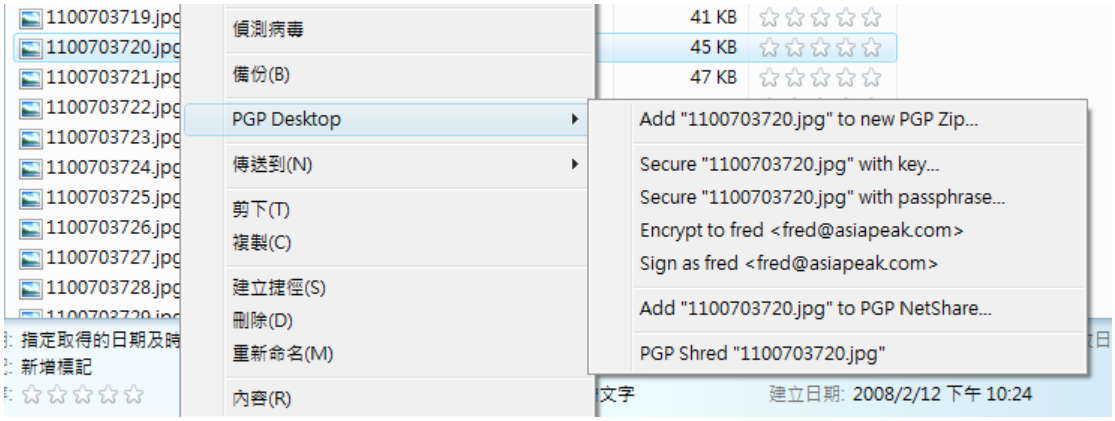


加過密的資料就如下圖所示，再把它貼到 eMail 裡寄出即可。



如果你只是要附件檔加密，例如一張自拍照(圖檔)，或是研發中的 CAD/CAM 檔，或是一般機密的 Office 檔案，你可以直接在檔案總管下按滑鼠右鍵，選擇[PGP Desktop]，然後選舉 [Secure … with key…]，PGP 視窗跳出讓你選擇可解開此加密檔的人(金鑰)，這檔案就被加密起來。萬一你不小心寄錯人了，因為此收件人不

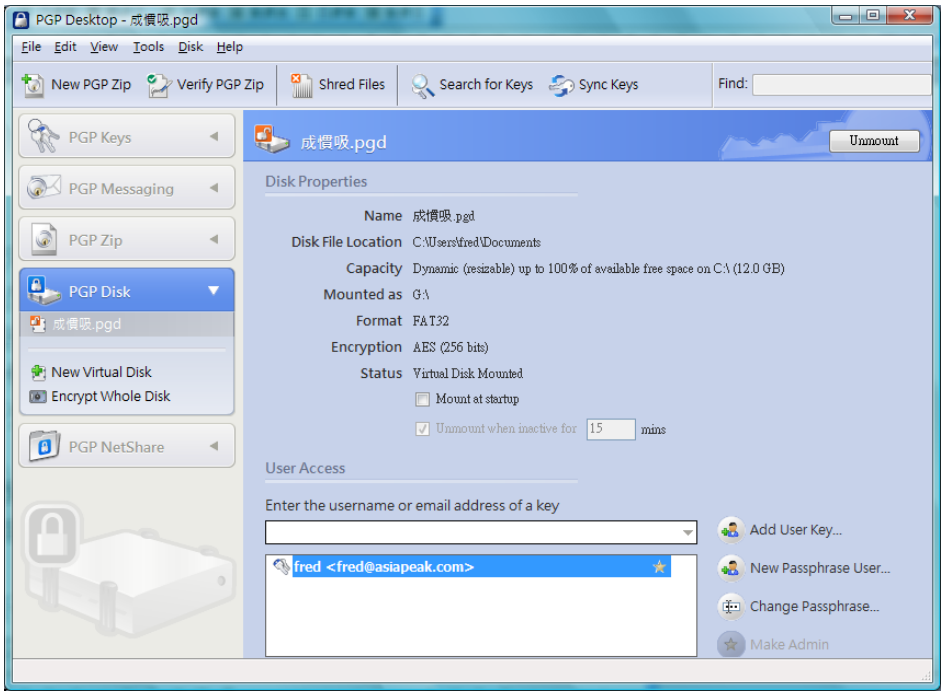
在你選擇的解密人名單裡，他也無法打開它。



PGP 使用技巧二：利用虛擬磁碟機(Virtual Disk)

如果您只是想要加密電腦裡的私密資料，除了您本人(或加上您指定的人)沒有其人可以解密這些資料。所以即使電腦遺失、電腦被盜用、甚或檢調單位來搜，也不用擔心這些私密資料外洩。通常，最安全的方法伴隨的是不方便使用，但是 PGP 的虛擬磁碟機加密功能可以安全又好用。

您可以指定硬碟某空間來做為一加密磁碟機，在這磁碟機裡的檔案及資料夾都是加密過的，只有你自己或是被您指定可出示私鑰或使用者代號密碼才能解密這些資料。任何你認為機密的檔案都可以擺到裡面，加過密的磁碟其操作如同一般檔案總管，您依舊使用 Word, Excel, Photoshop 等套裝軟體或應用程式來打開它，完全不受影響，因為 PGP 自動處理進出這磁碟機的加解密工作。



MSN 及 Skype 等即時訊息軟體通常會將聊天記錄保留下來，這也成了許多捉姦的證據之一。試試看把這些聊天記錄的位置改到加密磁碟機裡。

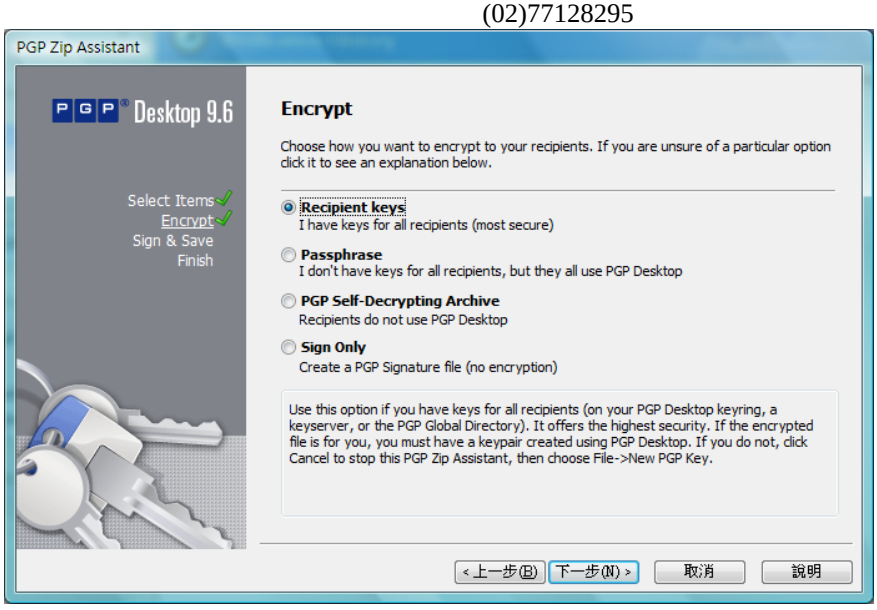
電子郵件軟體如 Outlook、Outlook Express 等，無論是收件匣或寄件備份，其實都是檔案而已，例如 Outlook 是.pst 檔，這些電子郵件檔案通常包括了很多機密內容。想想看，它們可不可能被人 Copy 走呢?

PGP 使用技巧三：檔案加密與壓縮功能

如果你只是想將部份目錄或檔案加密然後傳給別人(eMail 或 FTP 等)，你當然可以用 WinZip 或 WinRAR 等工具裡的密碼保護，但其加密演算法較弱，同時密碼也可能被猜到，這對於要傳送極機密的檔案資料是有風險的。PGP 則提供較高安全的類似工具，如果對方有 PGP，你應該使用對方的公鑰來加密，如果要將加密檔送給多人，就加入多個公鑰，擁有任何一個公鑰所對應的私鑰可以解密這些檔案，這是使用 RSA 2048 bit 加密演算法(內定)，所以比較安全；加完密後再用自己的私鑰來簽章，PGP 同時幫你將檔案壓縮。

如果對方沒有 PGP 時，你可以使用 Self-Decrypting Archive(SDA)，PGP 會要求你輸入加密密碼，然後使用這密碼來加密檔案，並產生可自動解密的執行檔，當然，您必須另外告知對方解密的密碼。

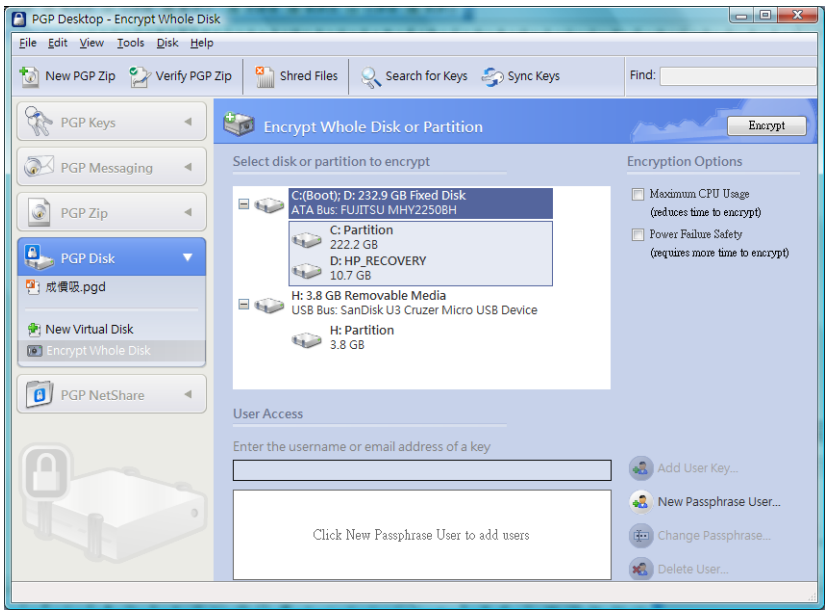
玉山科技股份有限公司
http://www.asiapeak.com
(02)77128295



PGP 使用技巧四：整顆硬碟加密(Whole Disk Encryption,WDE)

大部份人都知道，Windows 的登入密碼只是防君子不防小人的。當你的電腦遺失時，「撿到的人」可以用別的方式開機進入你的電腦看硬碟內容，對於安全要求比較高的某些人來說，只有檔案加密可能還是不夠。另外，隨身碟是最容易搞丟的東西，一不小心，重要資料就落入競爭者手中。

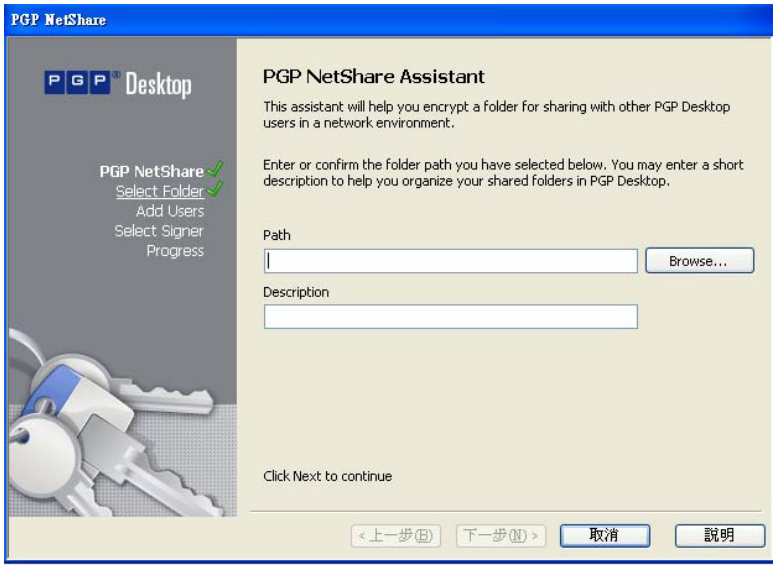
PGP 全硬碟加密可以針對隨身碟、外接式硬碟、硬碟 Partition、整顆硬碟加密。硬碟加密是將所有磁區都亂碼化(加密)，必須經過另一道驗證手續才能還原。如果是整顆硬碟加密，在開機時(Boot)會要求另外輸入密碼(或插入 USB Token)，如果是外接硬碟或 Partition 加密，則可使用 PGP 金鑰還原。



玉山科技股份有限公司
http://www.asiapeak.com
(02)77128295

PGP 使用技巧五：網路磁碟加密

以上所談都限於個人使用的電腦(Desktop & Notebook)，如果是工作群組使用的檔案伺服器或共享資料夾要如何保護及加密呢? 你當然可以花大筆銀子建立一套 PKI-like 的安全系統，雖然安全但很不好用。PGP NetShare 是一個容易使用的加密工具，加密網路磁碟就如同加密本機磁碟一樣，首先選擇共享資料夾路逕，再選擇允許解密這資料夾的使用者公鑰，然後選擇是否要簽章(證明這事是你做的)，PGP 就將你所選擇的資料夾加密，只有被授權的使用者(擁有被選定之公鑰對應之私鑰者)才能看到裡面的內容。



PGP 使用技巧六：徹底刪除資料

你一定知道， Windows 的刪除檔案的動作並不是真的從磁碟裡抹除，它只是被丟到「資源回收桶」，可以隨時再取回來。你可能也知道，按[shift]鍵再 Delete 時，Windows 會問你是否要永久刪除檔案，但這真的刪除了嗎? 隨便找一個反刪除或檔案救回工具軟體，如 FinalData，都可以再把檔案找回來；即使是格式化(Format)，尤其是快速格式化，都不見得可以完全將檔案從磁碟裡抹除，何況你不會只為了徹底刪除幾個檔案就要將硬碟整個 Format 吧!

PGP Shredder 工具可以將檔案內容完全抹除，即使你使用 FinalData 等工具要來找回檔案，可能看得到檔案名稱，可是內容絕對是一堆無意義的亂碼。使用 PGP Shredder 很容易，將要刪除的檔案拖放到桌面的 PGP Shredder Icon，或是直接在檔案總管按滑鼠右鍵，再選擇[PGP Desktop] [PGP Shred 這個檔案]即可。

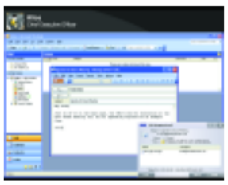
結論

最後，企業使用資料加密時還會關心一個問題：如果員工離職，如何解開他電腦裡的加密檔案? 或是如果您的私鑰遺失，或密碼忘了，是否就沒救了? PGP 有個專利技術，ADK(Additional Decrypting Key)，好好保管這支鑰匙。

對了，如果您是使用 Apple Mac 機器，PGP Desktop 也支援 Mac OS 的作業系統，而且操作方式與界面與 Windows 是一樣的。

資訊安全是沒有滿分的，對於個人電腦環境(Desktop)與點對點(End-to-End)的資料安全的需求來說，PGP Desktop工具是不錯的選擇。PGP 有 30 天完整功能試用版，可從原廠網站下載(http://www.pgp.com/downloads/desktoptrial2.php)。台灣授權代理商是玉山科技(http://www.asiapeak.com/pgp.php)。

PGP Desktop Email 9.6



Vendor	PGP Corporation
Price	$62 per user/year
Contact	www.pgp.com

PGP Corporation has been at the top of the market in email protection ever since it was first introduced as freeware in 1991. Since then it has matured, had several owners and now has its own home again. The results over the past two years have been excellent. PGP Corporation has kept the problem of encryption to about as transparent a process as we can imagine given that there needs to be at least some user intervention.

SC MAGAZINE BEST BUY

PGP Desktop Email is a bundle of encryption products in a single package. Among those is email encryption. When one buys the product, the license key activates the software for only those features purchased. Feature sets are easy to upgrade. Simply purchasing the new features — whole disk encryption, for example — causes a new key to be generated. Simply insert the new key in place of the old one and the product is upgraded. There is no need to reinstall. In fact, we attempted a reinstall over a previous installation of whole disk encryption and the product refused our efforts with no damage to the existing installation.

The product is simplicity itself to use. Once installation is complete, including a very simple key generation process, the product is ready to configure. This is done through policies that dictate the behavior of the encryption and digital signing to the granularity of an individual recipient if desired. Broader policies are equally simple to implement. For example, a policy that says "sign all email by default" signs transparently to the user, including caching the user's key at start up.

Documentation is as one would expect from PGP Corporation, very good. There is a short but comprehensive quick start guide and additional documentation is available on the PGP website. There is a variety of support options for users of most types — from individuals to small businesses and larger entities. The support portal is quite complete.

Priced starting at $62 per user per year, PGP Desktop Email is a good value. However, for true enterprise use it requires PGP Universal™ Server at an additional cost. PGP Universal Server allows full corporate management of all PGP encryption applications.

SC MAGAZINE RATING	
Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★
OVERALL RATING	★★★★★

Strengths A venerable product that behaves well and does exactly what it claims to do smoothly.
Weaknesses Can become a bit pricey in large enterprises. In this case, get the product package and get the product's full benefits.
Verdict A first rate product that fits into most environments cleanly. This product continues to set the standard for pure email security in an enterprise environment. We rate it our Best Buy.

A venerable product that behaves well and does exactly what it claims to do smoothly.

Peter Stephenson