



# **Mailsecurity**

for Exchange/SMTP

Email content/exploit  
checking & anti-virus

查閱電子郵件內容，探查侵犯 & 防電腦病毒



## GFI MailSecurity Exchange/SMTP 專用版

提供查閱電郵內容、探查侵犯、防電腦病毒及移除所有能影響用戶的危險電郵。



**Mailsecurity**  
for Exchange/SMTP  
Email content/exploit  
checking & anti-virus



## 目錄

- 電郵安全威脅
- 為何一個防電腦病毒軟件並不足夠
- 為何您需要多個防病毒驅動器
- 解決辦法：**GFI MailSecurity**
- 配置 **GFI MailSecurity**
- 電郵內容安全設定
- 創造內容檢查規則
- 附件檢查
- 電郵調節
- 病毒檢查
- 開發驅動器
- 特洛伊&執行檔案掃描器
- **GFI MailSecurity** 的新增功能
- 擴充性
- 測試您的電郵系統
- 推薦書
- 客戶名單
- 關於 **GFI**





## 電郵安全威脅

「2001年，電郵病毒「蠕蟲」及「特洛伊」導致全球高達132億美元的損失。」  
—電腦經濟，2002年一月

「被病毒侵襲的個案從2000年21,756宗增加到2001年52,658宗。」  
—CERT Coordination Center，2002年一月





## 為何一個防電腦病毒軟件並不足夠

「即使客戶應用的防電腦病毒軟件也不能阻止 ILOVEYOU 病毒進入... 這些軟件有可能會把正常的電郵誤當成病毒... 」

– *Messaging Today*, 2000年五月

「我知道許多人都認為電腦病毒掃描器是個解答，但我並不信任它們。ILOVEYOU，AnnaKournikova 或 Sircam 等病毒出現時，許多電腦病毒掃描器都不能對它們作出反應。」

– *Mark Minasi, Windows 2000 Magazine*, 2001年八月

您需要電郵內容安全系統！



## 爲何您需要多個病毒驅動器

1. 每個防電腦病毒軟件都有它們的強項和弱點。
2. 防電腦病毒軟件的製造者不能經常對新的病毒作出更新。
3. 一個防病毒驅動器意味著您只依賴一個防電腦病毒製造者。

多個防病毒驅動器 = 更強大的安全性！

請在這裡閱讀我們的白皮書：

[www.gfi.com/mailsecurity/wpmultiplevirusengines.htm](http://www.gfi.com/mailsecurity/wpmultiplevirusengines.htm)



## 解決辦法：GFI MailSecurity Exchange/SMTP 專用版

**GFI MailSecurity** 為 Exchange/SMTP 提供電郵內容檢查，剝削探測及防電腦病毒。它提供最好的 Exchange 及 SMTP 訊息掃描，配合：

- 多個病毒驅動器 - 適合病毒驅動器的獨立，更佳的安全性。
- 電郵內容及附件檢查 - 隔離危險的電郵。
- 剝削保護罩 - 偵查電郵闖入及防衛。
- 恐嚇電郵驅動器 - 分析及除去 HTML script、.exe 檔案等等。





## 配置 GFI MailSecurity 的三種方法:

1. 在 SMTP 網關模式設成郵件傳遞服務器 (電郵防火牆)。



2. 在 Exchange 2000 設 VS API 模式 - 掃描訊息貯備。



3. 兩者一起使用能提供最強大的安全性。



## GFI MailSecurity 檢查電郵爲了：

- 知名的電腦病毒
- 剝削
- HTML 郵件的 HTML scripts
- 危險的附件 - 例如 .exe 及 .vbs 檔案

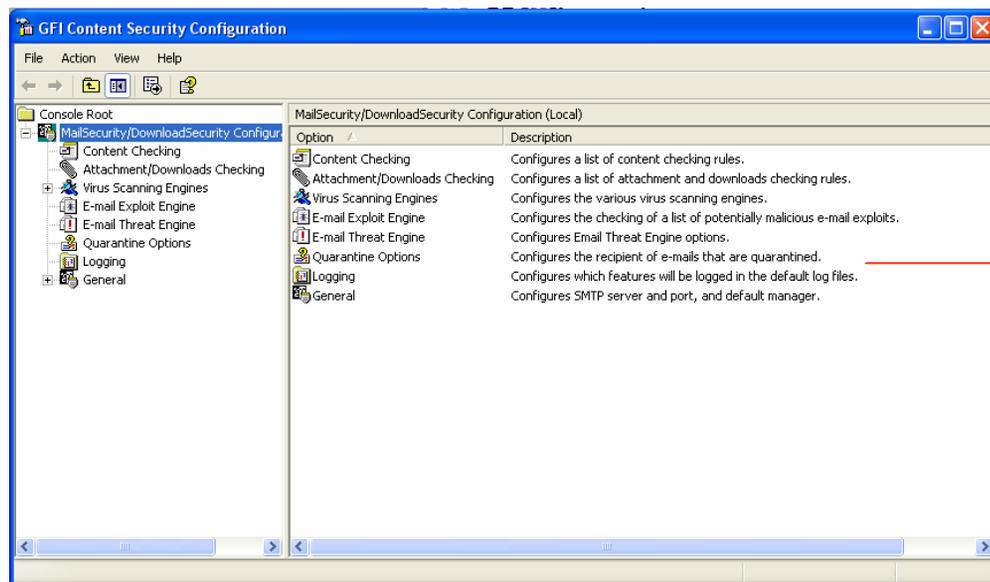


**GFI MailSecurity** 刪除知名的電腦病毒，使 HTML scripts失去能力及隔離那些管理員認爲可疑的電郵。



## 電郵內容安全設定

使用 **GFI MailSecurity**，您可以設定多樣的內容檢查及檔案檢查規則。



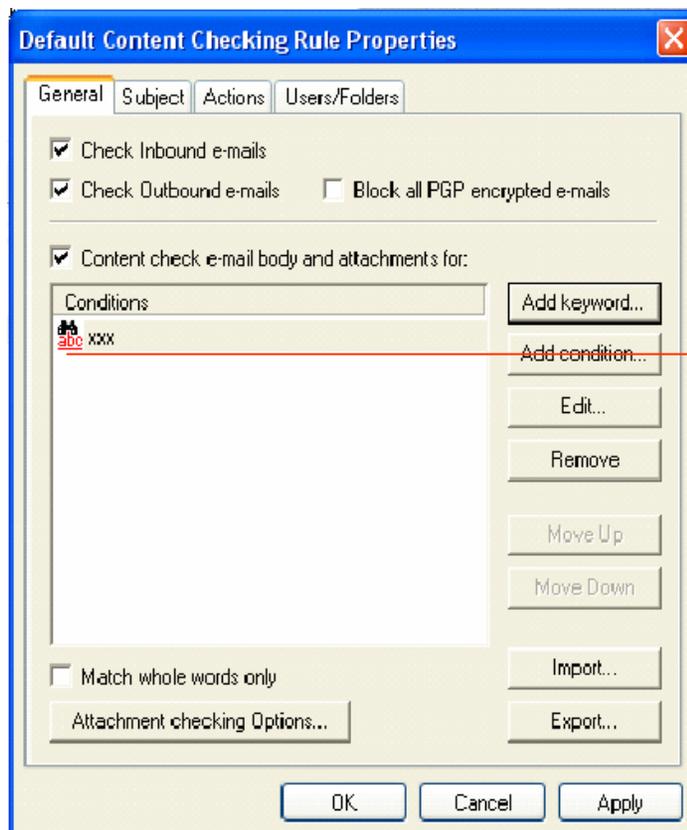
**GFI MailSecurity**  
配置

您可以創造多樣的內容檢查規則，使您能為不同的關鍵字、檔案類型及用戶設定不同的方針。



## 創造內容檢查規則 I

您可以創造新的內容檢查規則及指定檢查電郵的主題或主要內容的哪部分。



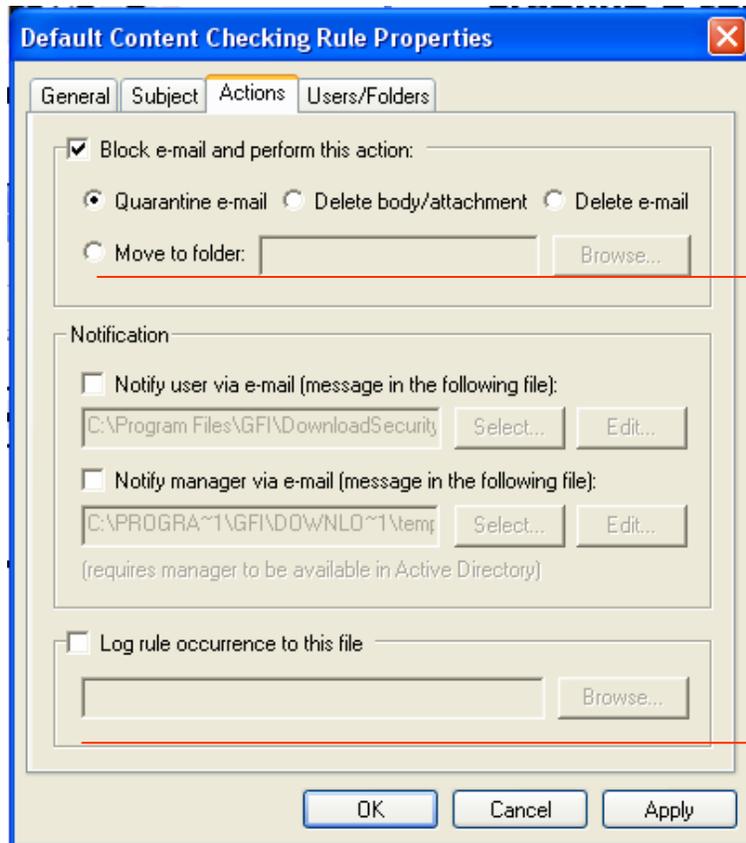
ailsecurity  
exchange/SMT  
content/ex  
king & ar

1. 為電郵的主要內容輸入檢查內容的關鍵字



## 創造內容檢查規則 II

現在指定怎樣處理那些電郵及給誰應用那些規則。



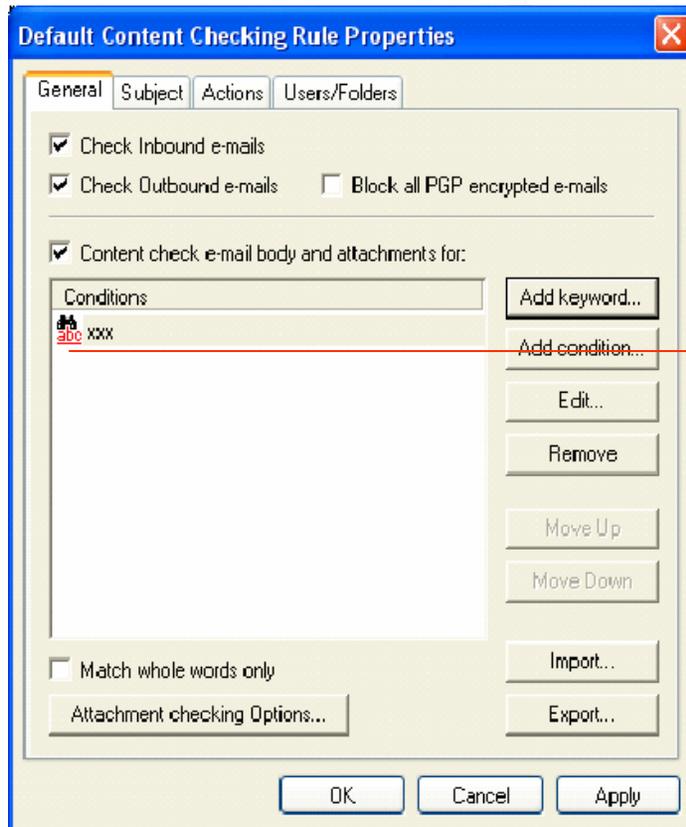
2. 隔離,刪除或移動電郵

3. 隨意地通報用戶及/或事件記錄



## 創造內容檢查規則 III

**GFI MailSecurity** 與活動姓名地址錄 (Active Directory) 的融合確保您能設定以用戶為基礎的規則。



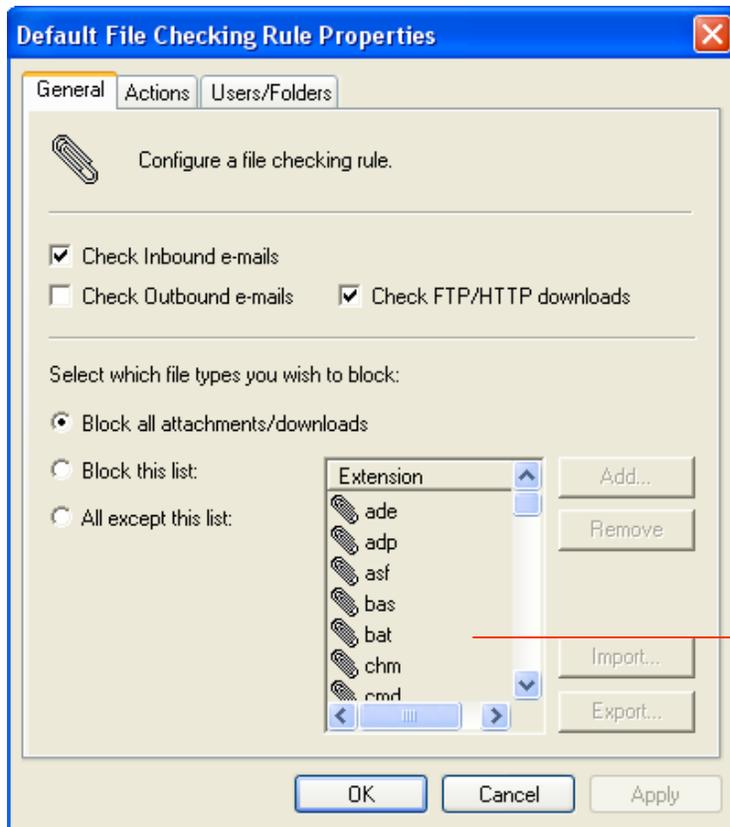
mailsecurity  
exchange/SMTP  
content/exploit  
ing & anti

應用內容檢查規則給一個或更多的用戶



## 附件檢查

您可以跟創造內容檢查規則的方法一樣創造附件檢查規則。



指定檢查哪種附件  
類型

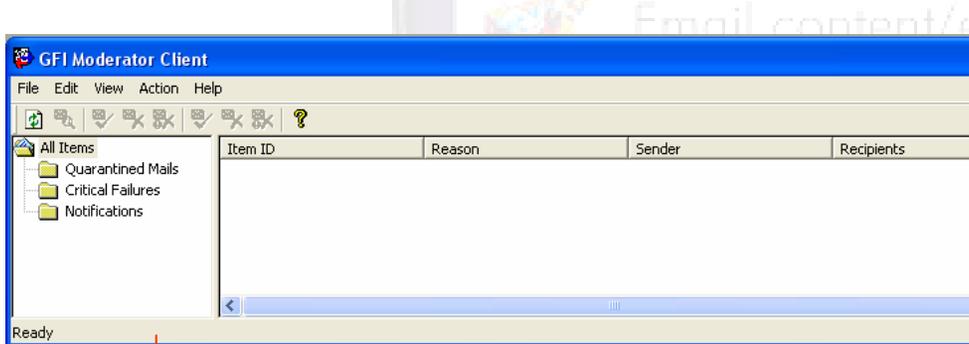


## 電郵調節

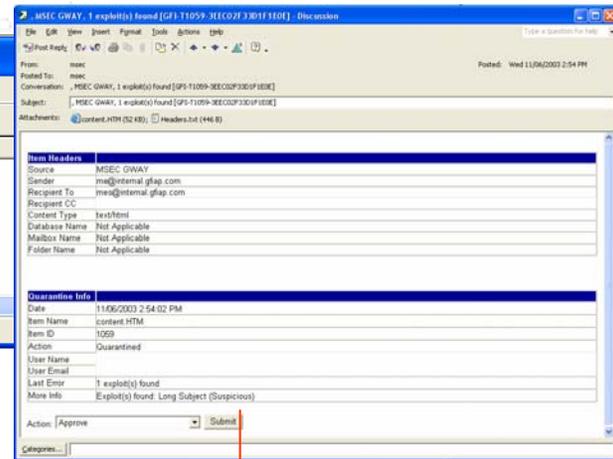
電郵一旦被隔離，它必須被批准或丟棄。

使用客戶調節器或電郵客戶能做到上述的功能。

您可以使用公用的文件夾分布管理的負載到多重的管理層。



使用客戶調節器



或經電郵客戶批准或丟棄



## 與多個病毒驅動器的病毒檢查

- **GFI MailSecurity** 是個獨立的病毒驅動器 - 它包含了多個防病毒驅動器，提供更強大的安全性。
- 包含 Norman Virus Control 及 BitDefender 病毒掃描驅動器。McAfee 病毒掃描驅動器可購買作為第三選擇。
- Norman 防病毒系統被 100% Virus Bulletin 授予 16 次優勝者。BitDefender 被 ICSA 鑒定為優良產品。



Awarded to Norman Virus Engine

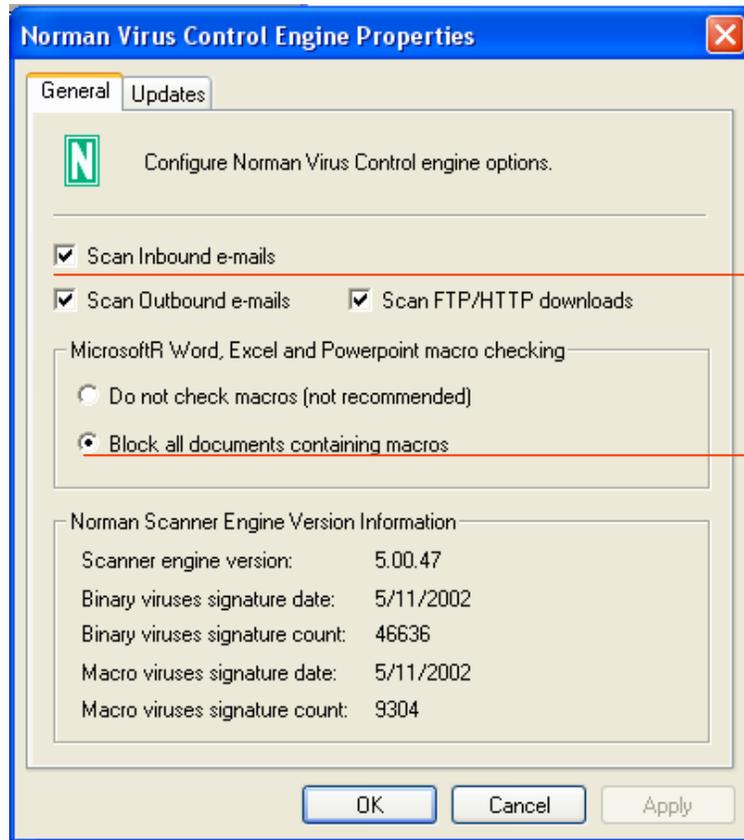


Awarded to BitDefender Virus Engine



## 病毒檢查設定

**GFI MailSecurity** 支援自動更新簽名文件。



mailsecurity  
change/SMTP  
content/exploit  
ing & anti-virus

按這裡啓動病毒掃描

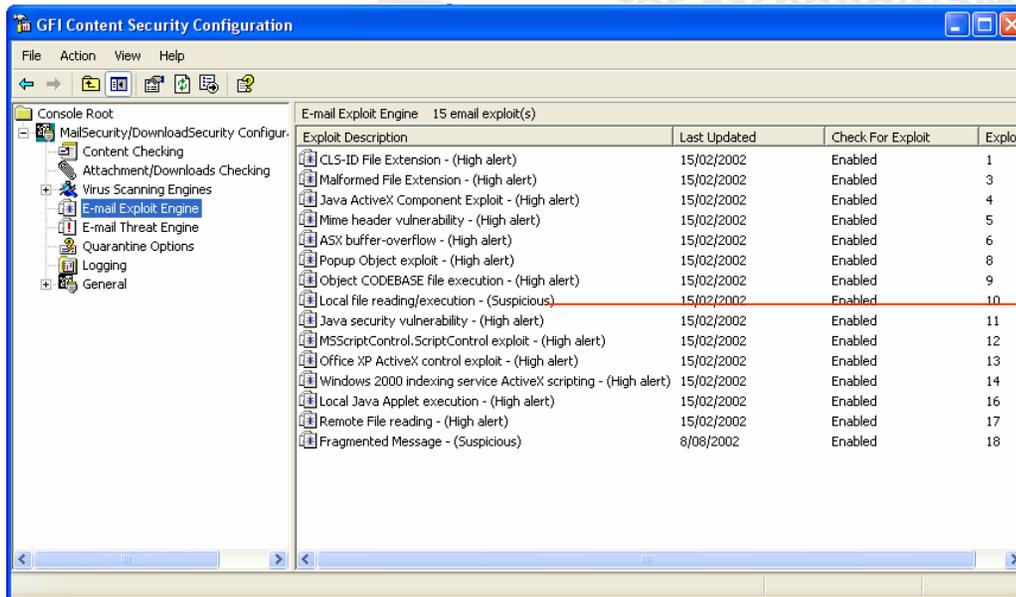
您可以在這裡選擇自  
動移除所有 Office  
macros



## 電郵開發驅動器

開發用途分辨出應用程序或操作系統的弱點後能執行程序/編碼或圍繞安全量度標準。

電郵開發是個內含在電郵的開發，當用戶打開或接收電郵時，它能在容納者的電腦上執行。



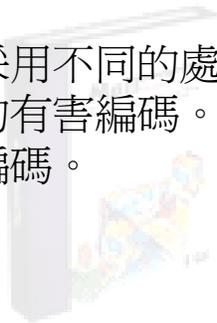
開發驅動器設定



## 爲何您需要開發驅動器

防電腦病毒軟體的構思是探測知名的有害編碼。

電郵開發驅動器采用不同的處理方法：它好像一個防經電郵闖入的探測系統 (IDS) 及分析那些可剝削的有害編碼。因此它能防護新的電腦病毒，但最重要是能防護知名的電腦病毒或有害編碼。



Email content/exploit  
checking & anti-virus

請在這里閱讀我們的白皮書獲得更多資料：

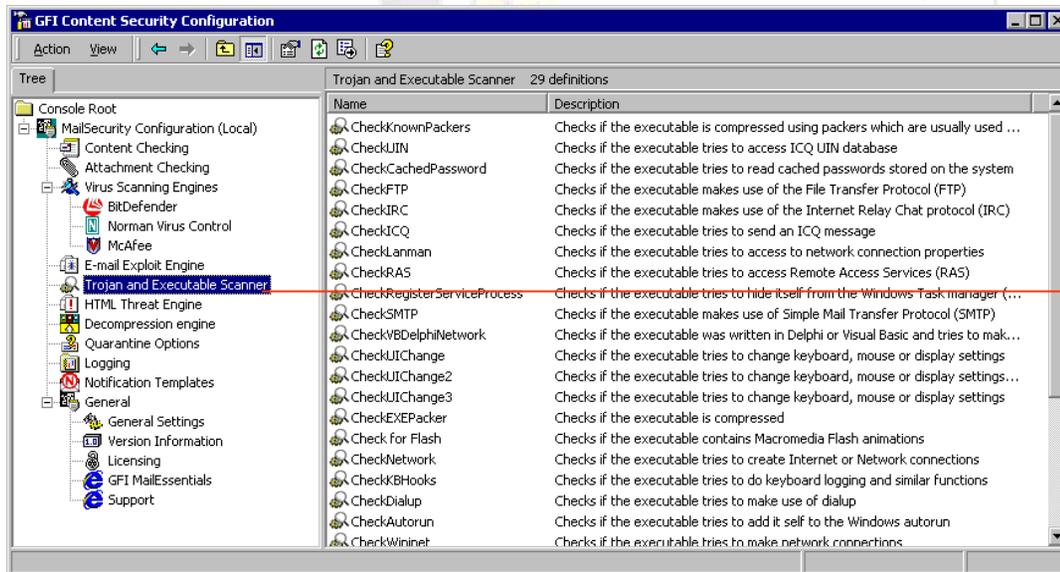
<http://www.gfi.com/mailsecurity/wpexploitengine.htm>



## 為何您需要特洛伊&執行檔案掃描器

特洛伊 (Trojan) 是一種電腦病毒，此程式貌似合法而實際上起破壞作用，因此它能神不知鬼不覺地進入受害者的電腦內。一般以病毒特徵為基礎的防毒軟件不能捕捉那些不知名的特洛伊。

**GFI MailSecurity** 提供特洛伊&執行檔案掃描器能分析每個進入的執行檔案，從而偵查那些不知名並有害的執行檔案 (例如特洛伊)。



配置特洛伊&執行檔案掃描器



## GFI MailSecurity 的新增功能

GFI MailSecurity 提供以下新的功能：

- *解壓驅動器* - 當提供壓縮檔案存檔的配置操作時，可支援超過75種壓縮格式 (打破了同行的記錄)。
- *基於互聯網的調節器* - 確保管理員能經由瀏覽器調節被隔離的檔案。
- *經由 HTTP 下載修正/更新* - 避免防火牆配置的必要。修正/更新可經由姓名地址錄分發。
- *更多隔離的選項* - 被隔離的檔案可由連結代替附件發送給用戶。
- *支援 Exchange 2003 & 2000*。
- *支援 Windows 2000 & Windows 2003*。



## 擴充性

**GFI MailSecurity** 是唯一能支援 Exchange 2000 VS API 的內容檢查產品。VS API 是被 Microsoft 推薦為必需的應用編程接口！

SMTP 網關版本與 IIS5 的融合能平行速度及增強擴充性。





## GFI MailSecurity: 優惠的價格

**GFI MailSecurity\*** 是領導市場的內容檢查產品，全世界有超過 10,000 個服務器已安裝了本產品。

它提供無匹敵的價格。GFI 的定價比競爭者低 30%：

用戶數量	100	500	1,000
ScanMail Exchange 套裝	\$2,430	\$10,475	\$19,050
MIMEsweeper	\$3,233	\$8,664	\$12,277
GFI MailSecurity	\$ 1,495	\$ 3,500	\$ 4,995

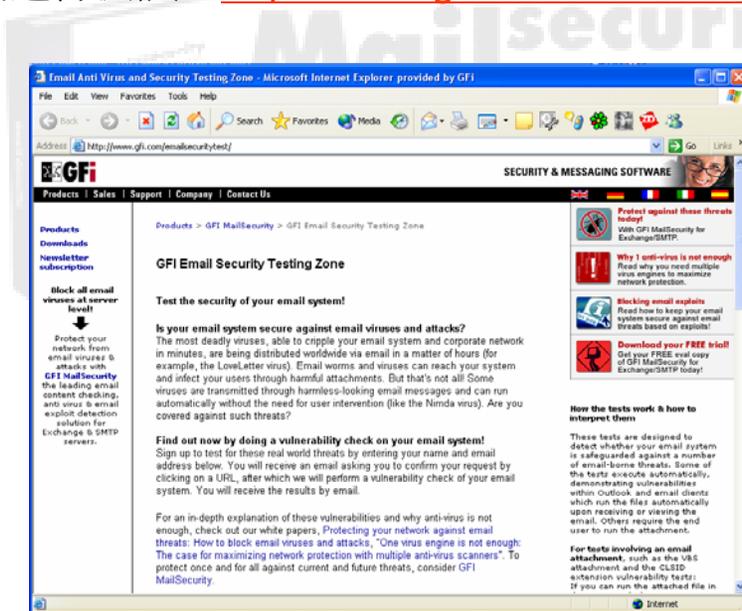
\*以前命名為 **Mail essentials**。



## 測試您的電郵系統是否易受恐嚇電郵的攻擊

您的郵件服務器是否容易受電郵病毒及剝削的攻擊？

使用 **GFI** 的網頁進行測試：<http://www.gfi.com/emailsecuritytest/>



在這里，您可以檢查當您的電郵系統面對包含被感染的電郵、畸形的 MIME 標題的電郵、內含的 script 的 HTML 電郵等威脅的時候，它是否安全可靠。



## 推薦書

「三年前，我們開始使用 **GFI MailSecurity** 及它的前任產品，**Mail essentials** 來防礙不必要及危險的附件。我不能想象一個電郵服務器可在缺少它的情況下運行。」

- *Joe Stern, Director of IT, National Analysts, Inc., 費城, PA, 美國*

「**GFI MailSecurity** 保護我們每日來自所有病毒的侵襲，它們十分可怕！」

- *Charlie Wiley, IT Director, Dixie Iron Works, Ltd, Alice, TX, 美國*

「我們已經使用 **GFI MailSecurity** 超過了兩年。在這期間我們從沒有感染過病毒，許多病毒都已被 **GFI MailSecurity** 捕捉。它的管理程序十分容易及快捷。」

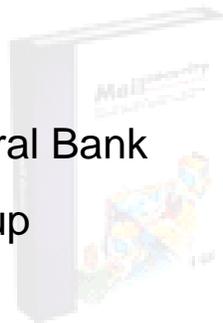
- *Paula Chesbrough S.V.P., Eagle Bank, Everett, MA, 美國*



## 客戶名單

多間大型公司於世界各地均使用 **Mail essentials**，他們包括：

- NASA
- European Central Bank
- MG Rover Group
- Caterpillar
- PerotSystems
- Port Of Tilbury London Ltd
- Mexx International BV (Netherlands)
- and many more



Mailsecurity  
for Exchange/SMTP  
Email content/exploit  
checking & an





## 下載

從這裡下載 **GFI MailSecurity Exchange/SMTP** 專用版的免費拷貝：

<http://www.gfi.com/downloads/downloads.asp?pid=4&lid=1>

請瀏覽這裡獲得關於電郵剝削內容檢查、防電腦病毒、及其他電郵安全問題的白皮書：

<http://www.gfi.com/mailsecurity/msecpapers.htm>



## 關於 GFI

- **GFI** 分別在美國、英國、德國、澳大利亞及馬耳他設有辦公室，及擁有全球性的經銷商網絡。
- **GFI** 是個領導 **GFI FAXmaker**、**GFI MailSecurity**、**GFI MailEssentials** 及 **GFI LANguard** 產品行列的市場開發者。
- **GFI** 榮獲美國微軟公司 2000年最佳應用軟件伙伴冠軍。
- 請瀏覽 [www.gfi.com](http://www.gfi.com) 取得更多資料。