

2016

勒索軟體白皮書



| 目 錄

什麼是勒索軟體	1
勒索軟體的歷史	1
勒索軟體的流行原因	2
勒索軟體所造成影響	2
勒索軟體的製作成本極低	5
勒索軟體的傳播途徑	
網路釣魚郵件	5
惡意廣告	6
網頁掛馬	9
Botnet	10
先滲透再攻擊	11
主動橫向感染	11
您或公司具備足夠防護了嗎？勒索軟體防治檢核清單	
政策面	11
技術面	12
傳統防毒	12
網路釣魚郵件	12
惡意廣告 網頁掛馬	12
Botnet	12
滲透攻擊與主動橫向感染	12
檔案備份與復原	13
趨勢科技勒索軟體防禦產品一覽表	14



2016勒索軟體白皮書

什麼是勒索軟體

勒索軟體是一種讓受害者不能夠存取他們電腦的惡意軟體。它的目的是要威脅受害者付出贖金來讓系統或資料復原。勒索軟體分成兩種，一種是加密型勒索軟體，另外一種是限制系統運作的勒索軟體（例如將受害者系統鎖住，除了付贖金之外，不能做其他動作）。

勒索軟體的歷史

根據維基百科的描述，第一個勒索軟體是出現在1989年的AIDS木馬，AIDS木馬會將C槽的目錄隱藏，把檔名加密，要求受害者付出美金189元來重新更新授權。之後勒索軟體便沈寂了很長一段時間。

直到2005至2006年間，比較精密的勒索軟體才再度出現，便是TROJ_CRYPTZIP.A，它會搜尋受害者硬碟上某些副檔名的檔案，將這些檔案壓縮成含有密碼保護的壓縮檔，再將原始檔刪除。

2011年的TROJ_RANSOM.QOWA是屬於限制系統存取的勒索軟體，他會把使用者電腦鎖住，得撥打付費電話支付12美元才能解鎖。2012年的RENETON開始假冒當地警察，讓使用者以為自己做了違法的事情，所以必須付出罰款。同時也做在地化，會追蹤使用者的位置，出現當地的執法機關的標誌，受害者遍及歐洲跟美國。

2013年出現了當時最危險的Cryptolocker，此勒索軟體除了把整台電腦鎖住之外，也會將檔案加密，Cryptolocker使用了AES配上RSA的加密演算法，讓使用者無法還原檔案。而Cryptolocker要求的贖金高達300美元。此時勒索軟體的散布方式演進成使用垃圾郵

件來散布。

2014至2015年間，開始出現了利用比特幣來支付贖金的勒索軟體TROJ_CRYPTRBIT.H，勒索軟體陸陸續續也出現了各種「進化」，像是利用Tor網路來隱藏自己行蹤的CTBLocker，以及利用e-mail誘導使用者進入偽造官方網頁，並要求輸入驗證碼來下載檔案的TorrentLocker。也開始出現針對企業機構的勒索軟體，像是Ransomweb會把網站和網站伺服器加密，而Chimera勒索軟體則除了加密檔案之外，還威脅使用者如果不付贖金，就會將檔案公開在網路上。在行動裝置方面，也出現了針對Android手機的勒索軟體。

2016年，出現了針對Mac OSX的勒索軟體KeRanger，勒索軟體也開始對醫院造成重大影響，像是Locky造成醫院緊急將所有電腦關機，改用紙本作業；SamSam則是藉由攻擊伺服器的漏洞來散布，主要攻擊目標也為醫療產業。

勒索軟體的流行原因

勒索軟體最終的目的是從中得利，所以金流一向是勒索軟體所重視的，金流必須具有匿名性而且可靠，2009年出現的比特幣剛好符合這個特性。勒索軟體作者不再需要使用預付卡這類的付款機制，而是可以直接透過網路匿名交易比特幣來獲取不法收益，最重要的是，很難發現他們的行蹤。而當惡意駭客發現使用勒索軟體的獲利能力很高時，便大量撰寫勒索軟體來增加收益，部分更開始經營勒索軟體服務。

勒索軟體所造成影響

勒索軟體分為兩種，一種是限制系統運作類型，另一種則是現在最流行的檔案加密類型，造成影響分別如下：

■ 限制系統運作類型

駭客讓使用者無法正常使用電腦，直到使用者付出贖金，才能正常使用系統，這種類型不是對檔案加密，而是鎖住電腦。

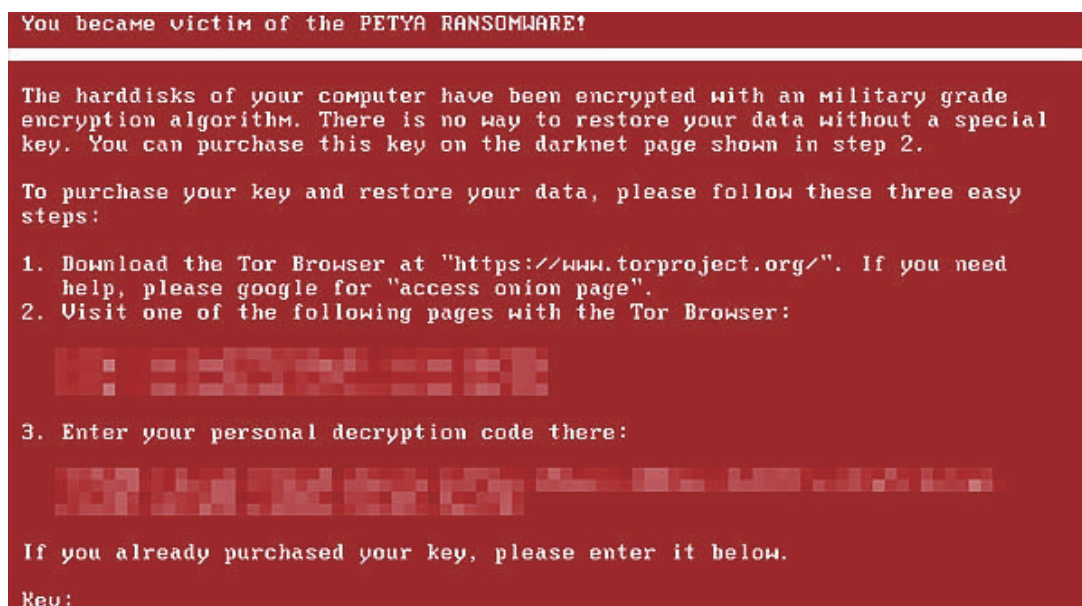
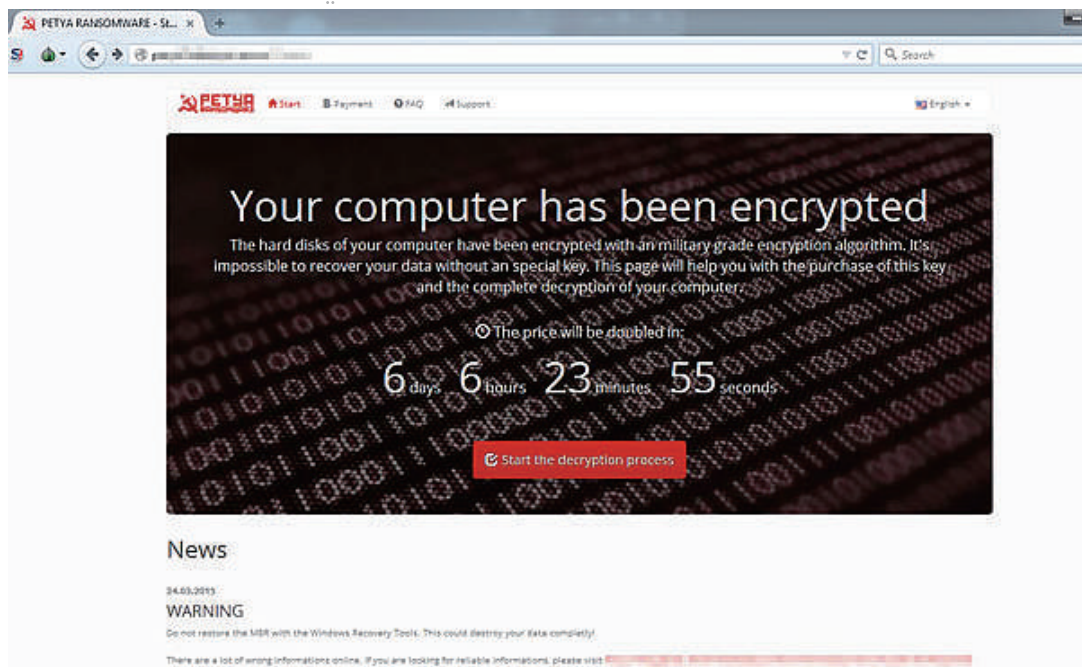
■ 檔案加密類型

駭客會針對目標檔案使用加密演算法進行加密，多為文件與影音照片，讓使用者無法開啟自己的檔案，由於文件與影音照片對大部分使用者的價值較高，所以願意付出贖金的意願也會更大。

不過，隨著勒索軟體的演進，近期也開始看到針對MBR與MFT加密的勒索軟體（例如：PETYA），這類的勒索軟體不是針對檔案做加密，而是直接對整個磁碟做加密，當使用者重開機時，被竄改過的MBR便會讓使用者看到勒索畫面，而無法順利進入作業系統。

根據FBI在2015年公布的報告^{*1}，典型的勒索軟體要求的贖金範圍在200美金到1萬美金之間。

CryptoWall 3.0的中毒畫面



PETYA勒索病毒的中毒畫面

勒索軟體的製作成本極低

根據ICIT的調查報告^{*2}，架設釣魚網站以及發送釣魚郵件的成本約為5,000元台幣，從地下組織購買一個勒索軟體約為65,000元台幣，而每個願意付贖金的受害者平均願付出10,000元贖金。只要約7到8位受害者付出贖金後，勒索軟體就開始賺取利益。

勒索軟體的傳播途徑

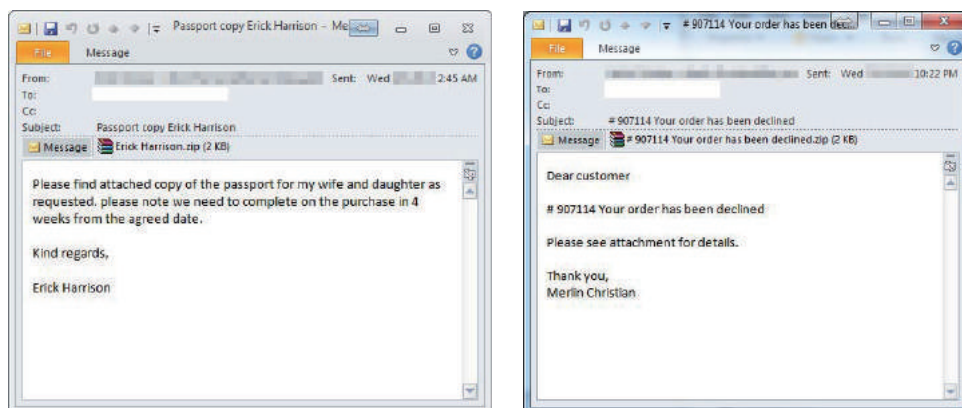
■ 網路釣魚郵件

根據調查，絕大部分收到勒索軟體入侵的原因都是誤點了網路釣魚郵件，大部分的網路釣魚郵件內容可以區分成幾種類型：

- (1) 快遞或郵寄通知
- (2) 帳單或訂單
- (3) 應徵者履歷
- (4) 退稅，發票或罰單

大部分的釣魚郵件都會將執行檔偽裝成文件檔案，當使用者一旦雙擊文件，勒索軟體便會開始加密使用者的文件。近期內，也發現直接利用應用程式的漏洞或是巨集來攻擊，並下載勒索軟體，例如說勒索軟體Locky。

另外一種常見手法則是在釣魚郵件內放入惡意網站的網址，當使用者點擊連結後，便會遭受攻擊並下載勒索軟體。



勒索軟體的釣魚信件範例

■ 惡意廣告

大多數人對於惡意廣告存在著很大的誤解，以為一定要點擊才會受到危害，事實上，惡意廣告的攻擊並不需要使用者點擊，只要瀏覽器或裝置顯示出惡意廣告，使用者就會受到攻擊。惡意廣告的攻擊可以分成兩種類型：

(1) 點擊前(Pre-Click)攻擊

在使用者瀏覽網頁時，惡意廣告可以透過軟體漏洞來攻擊，例如Java, Flash Player 甚至是瀏覽器漏洞。也可以透過廣告系統的弱點，撰寫script來發動主動攻擊，勒索軟體可以在使用者僅單純瀏覽網頁的情況下，就進行攻擊。

(2) 點擊後(Post-Click)攻擊

這是惡意廣告中最經典的情境。當使用者點擊惡意廣告時，便會被導向一個攻擊者所建置的惡意網站，裡面存放著攻擊的程式，當使用者看到惡意網站時，就有機會開始執行惡意程式。

Pre-click 惡意廣告

01

使用者未更新程式

e.g. 使用舊版Flash Player



02

利用Flash的漏洞

使用者瀏覽正常網頁，
但廣告正好輪播到惡意廣告



03

Flash惡意廣告

Flash惡意廣告會試著攻擊以取得系統管理者權限，一旦成功，便會利用系統管理者權限下載Downloader並執行

註：一般來說，惡意軟體會先下載Downloader，此Downloader檔案大小較小，目的通常單純。



+ Flash惡意廣告



取得權限



下載Downloader



執行Downloader

04

Downloader被執行後，便會下載完整的勒索軟體並執行。
勒索軟體一旦執行，使用者的檔案就會被加密。



下載勒索軟體



執行勒索軟體



檔案加密

Post-click 惡意廣告

01

建立惡意網站

駭客先建立一個惡意網站
裡面存放攻擊程式



02

駭客建立惡意廣告， 導向惡意網站



03

使用者看到惡意廣告並點擊，
此時使用者便會被導向惡意網站



04

使用者瀏覽惡意網站的同時，
便遭受攻擊，下載Downloader
並執行



- ① 取得權限
- ② 1. 下載Downloader
2. 執行Downloader

05

Downloader被執行後，便會下載完整的勒索軟體並執行。
勒索軟體一旦執行，使用者的檔案就會被加密。



下載勒索軟體



執行勒索軟體



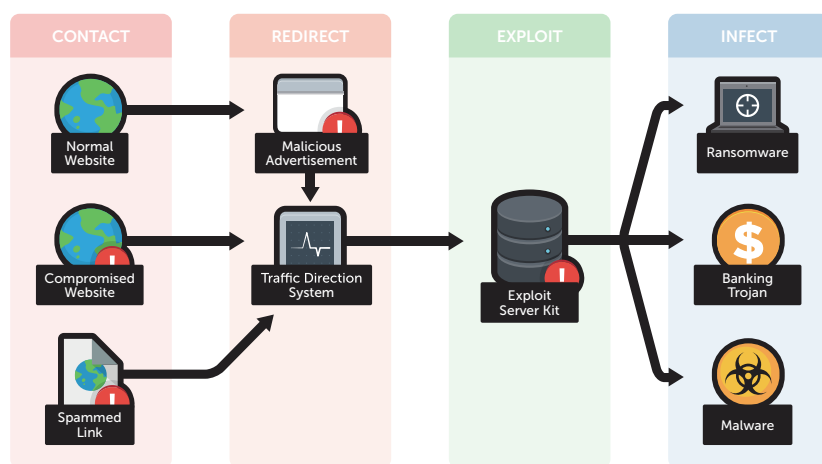
檔案加密

■ 網頁掛馬

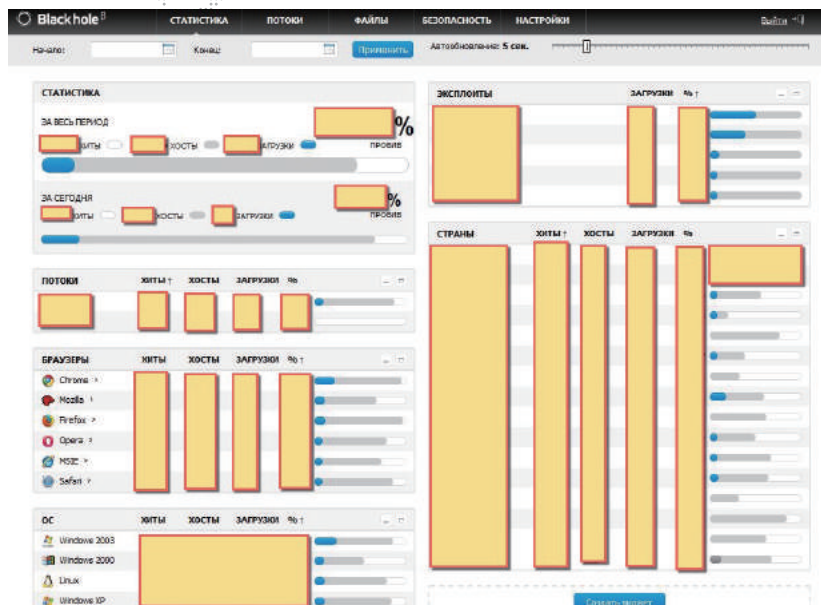
勒索軟體作者會透過入侵企業網站來達到散布勒索軟體的作用，當他們發現網站伺服器或是應用程式有安全性漏洞時，他們便會入侵並在網頁上放入script導向裝載「漏洞攻擊套件 (Exploit Kit)」的網頁，此時「漏洞攻擊套件」便會掃描使用者的漏洞來達到主動下載並執行勒索軟體的目的。



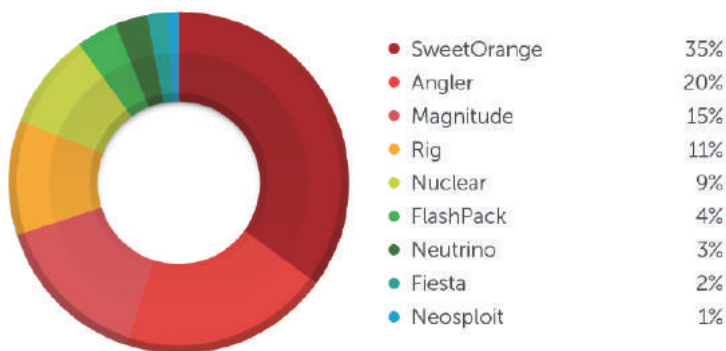
下圖為Exploit kit的基本攻擊流程，可以看到不管是使用者瀏覽一個帶有惡意廣告的普通網站，或是原本就是惡意的網站，都會被導向帶有Exploit Kit的伺服器，當Exploit Kit成功攻擊使用者的電腦，駭客就可以在使用者的電腦中種下勒索軟體或其它惡意程式。



Exploit kit的攻擊流程



Exploit kit Blackhole的控制台畫面



趨勢科技在2015年所偵測的Exploit kit家族分布圖

Botnet

由於勒索軟體的利潤高，所以很多提供Botnet的地下組織開始提供勒索軟體的服務(RaaS)，並且與購買的人分享利潤，一旦購買勒索軟體的服務，Botnet地下組織便會大量感染旗下控制的電腦，讓收益提高。

■ 先滲透再攻擊

勒索軟體LeChiffre是透過APT進入許多印度公司後，被手動執行起來。而勒索軟體Surprise則是透過TeamViewer的漏洞下載並執行。這種綜合式攻擊手法預期會越來越多。

勒索軟體SamSam是利用JexBoss來主動掃描使用JBoss的伺服器，當JBoss是有弱點的舊版本，就會被入侵並安裝勒索軟體。在這同時，也會主動橫向擴散，掃描網路上其他的JBoss伺服器。

■ 主動橫向感染

在手機上的勒索軟體Koler是透過Android手機簡訊漏洞來感染通訊錄上朋友的手機，勒索軟體LowLevel04則是透過遠端桌面的漏洞來橫向感染他人電腦。

您或公司具備足夠防護了嗎？勒索軟體防治檢核清單

■ 政策面

(1) 應定期確認所有主機(包含終端使用者以及伺服器主機)，都更新至最新安全性更新。

安全性更新分別為作業系統以及應用程式(例如Flash, Acrobat, Office, etc.)

- 微軟每月定期進行更新，須安排當月於測試環境驗測無誤後，進行更新。
- 其他第三方廠商之軟體，也應於弱點公布、廠商提供相關修補程式後，於當月安排時間進行更新。
- 定期檢閱CVE，以確認是否有新的弱點需要進行修補(每週/每月)。

(2) 訂定良好的網路共享權限管控

- 共享資料夾應明確指定共享帳號(或群組)

(3) 終端使用者以及伺服器主機存取Internet，應有良好的規範控管

- 針對伺服器，禁止下載可執行檔
- 針對伺服器，上網採用正向表列開放可存取網站
- 針對POS, Kiosk系統，採取正向表列可執行的程式。
- 針對終端使用者，禁止瀏覽高風險網站。

(4) 重要資料應定期備份，並且應於定期進行資料還原演練

- 備份應該在不影響日常運行，並且貼近於使用者平時使用習慣
- 重要資料應每週或每月進行備份
- 備份資料應於每季或每半年進行還原演練
- 備份應有一份離線備份，避免遭受感染時，一併感染備份的檔案

(5) 提高企業內部員工資訊安全意識

- 加強內部宣導，不要隨意開啟來源不明的郵件附加檔案(特別是.SCR, .CAB格式)
- 應定期針對內部員工進行資訊安全訓練(如每季)
- 於公司內公共場所提供資安訊息

■ 技術面

應持續更新作業系統或是應用軟體，平均四天軟體漏洞就可能被駭客所利用

(1) 傳統防毒

- 針對最新已知病毒可以有效隔離並刪除。
- 使用雲端防護機制，讓端點防護可以得到最快最新的保護。

(2) 網路釣魚郵件

- 公司安裝了可以防治惡意軟體的郵件攔道
- 公司郵件攔道可以使用沙箱來測試惡意軟體
- 不小心誤開啟惡意郵件後，端點防護軟體仍然可以偵測到可疑加密行為並中斷執行。

(3) 惡意廣告 網頁掛馬

- 使用網頁信譽評等相關雲端服務來阻隔已知惡意網頁
- 端點防護可以在勒索軟體與C&C伺服器溝通時有效阻隔
- 端點防護可以偵測到Exploit kit並阻擋

(4) Botnet

- 針對已知Botnet的C&C伺服器可以有效隔離
- 端點防護可以偵測Botnet是否在背景運作並阻擋
- 公司管理者可以透過系統偵測內部有可疑Botnet連線並阻擋

(5) 滲透攻擊與主動橫向感染

- 公司管理者可以透過系統發現可疑封包並阻擋

- 端點防護在未知勒索軟體執行時，能發現可疑加密行為，並在第一時間嘗試備份檔案；確定為惡意後可阻擋加密行為並阻擋勒索軟體，並有機會利用檔案備份復原檔案。

(6) 檔案備份與復原

- 遵守3-2-1備份原則：3份備份、2種不同儲存媒體、1個不同的存放地點。

資料來源：

*1：FBI, 2015 June,
<https://www.fbi.gov/sandiego/press-releases/2015/fbi-warns-public-of-cryptowall-ransomware-schemes>

*2：ICIT (Institute for Critical Infrastructure Technology), 2016 March,
<http://icitech.org/wp-content/uploads/2016/03/ICIT-Brief-The-Ransomware-Report2.pdf>

趨勢科技勒索軟體防禦產品一覽表

	重要 主機防護	間道防護端			內網分析功能		端點防護端		中央 控管	備份	雲端服務防護	
	Deep Security	IWSVA	IMSA	DDEI	DDI	DDAn	OSCE 11	WFP	TMCN	Safesync	Cloud App Security	Hosted Email Security
網路釣魚郵件												
安裝防治惡意軟體的郵件間道			○	○							○	○
郵件間道有沙箱功能來測試惡意軟體			☆	○		☆					○	○
誤開啟惡意郵件後，端點防護軟體仍然 可以偵測到可疑加密行為並中斷執行							○	○				
惡意廣告、網頁掛馬												
有網頁信譽評等功能的相關雲端服務可 阻隔已知惡意網頁	○	○					○	○			○	
端點防護可以有效阻隔在勒索軟體與C&C 伺服器之間的溝通	○	○					○	○				
端點防護可以偵測到Exploit kit並阻擋	○	○					○	○				
Botnet												
可以有效隔離已知Botnet的C&C伺服器	○	○					○	○				
端點防護可以偵測Botnet是否在背景運 作並阻擋	○						○	○				
管理者可以透過系統偵測內部可疑 Botnet連線並阻擋	○				○		○	○				
滲透攻擊與主動橫向感染												
管理者可以透過系統發現可疑封包並阻擋					☆		☆		☆			
端點防護在未知勒索軟體執行時，可以 發現可疑行為，同時在第一時間嘗試備 份檔案；確定為惡意後阻擋加密行為並 阻擋勒索軟體，並有機會利用檔案備份 復原檔案							○	○				
檔案備份與復原												
檔案一旦改變，可以隨時備份										○		
可以任選目錄備份，不須改變使用行為										○		
有版本控制，可恢復之前版本										○		
重要伺服器防護												
主動察覺公司重要主機的檔案或是應用程 式遭受到入侵或是異常變動，並提供分析 報表	○											
定期更新修補程式造成的漏洞												

☆：同一行中標示為☆的產品需要互為搭配，方具有此一功能

