以加密勒索軟體為例，拆解網路攻擊鏈—最佳化端點、電郵與網頁防護實務

保安資訊有限公司 陳炳銘 顧問

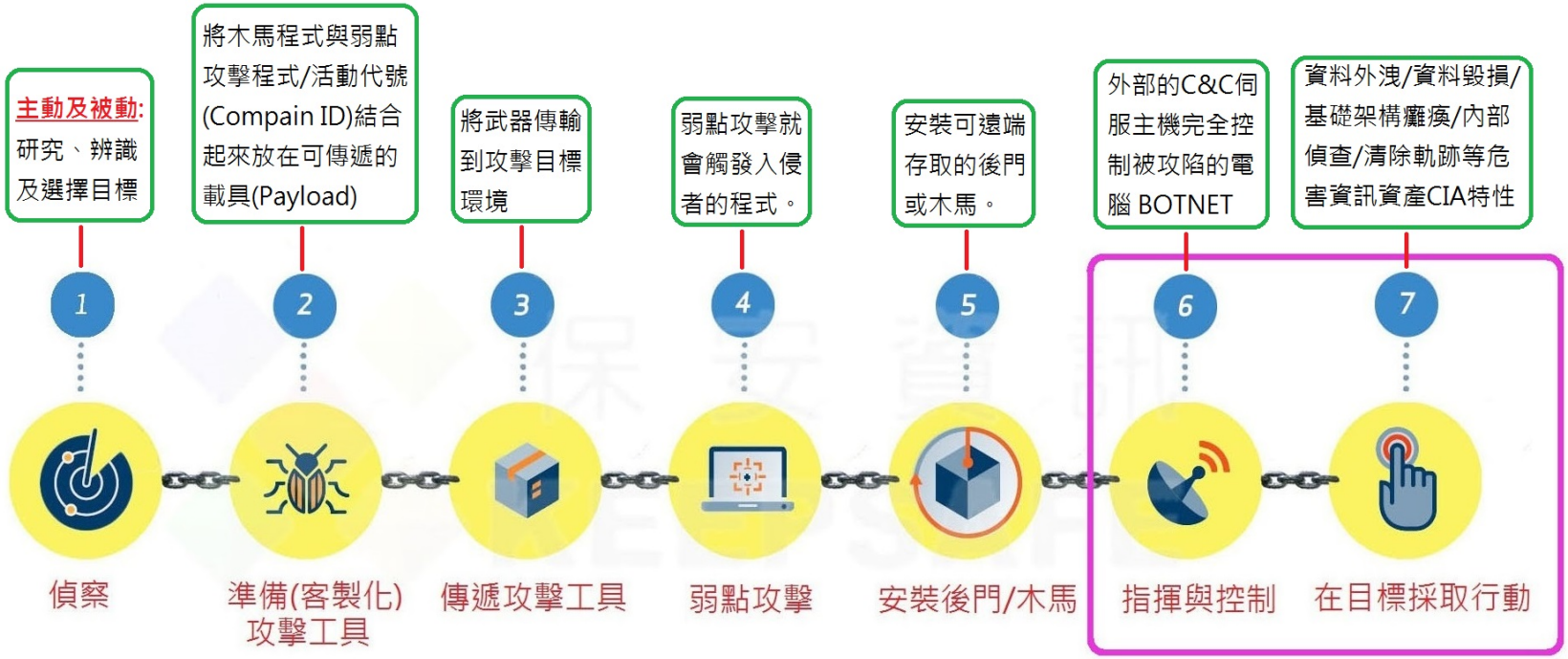
www.SaveTime.com.tw 好記:幫您節省時間.的公司.在台灣

We Keep IT Safe，Secure & Save you Time，Cost

“知己知彼，百戰百勝”-拆解網路攻擊模式:以洛克希德馬丁公司的網路攻擊鏈(Cyber Kill Chain)框架

保安資訊 SAVETIME INFORMATION SECURITY

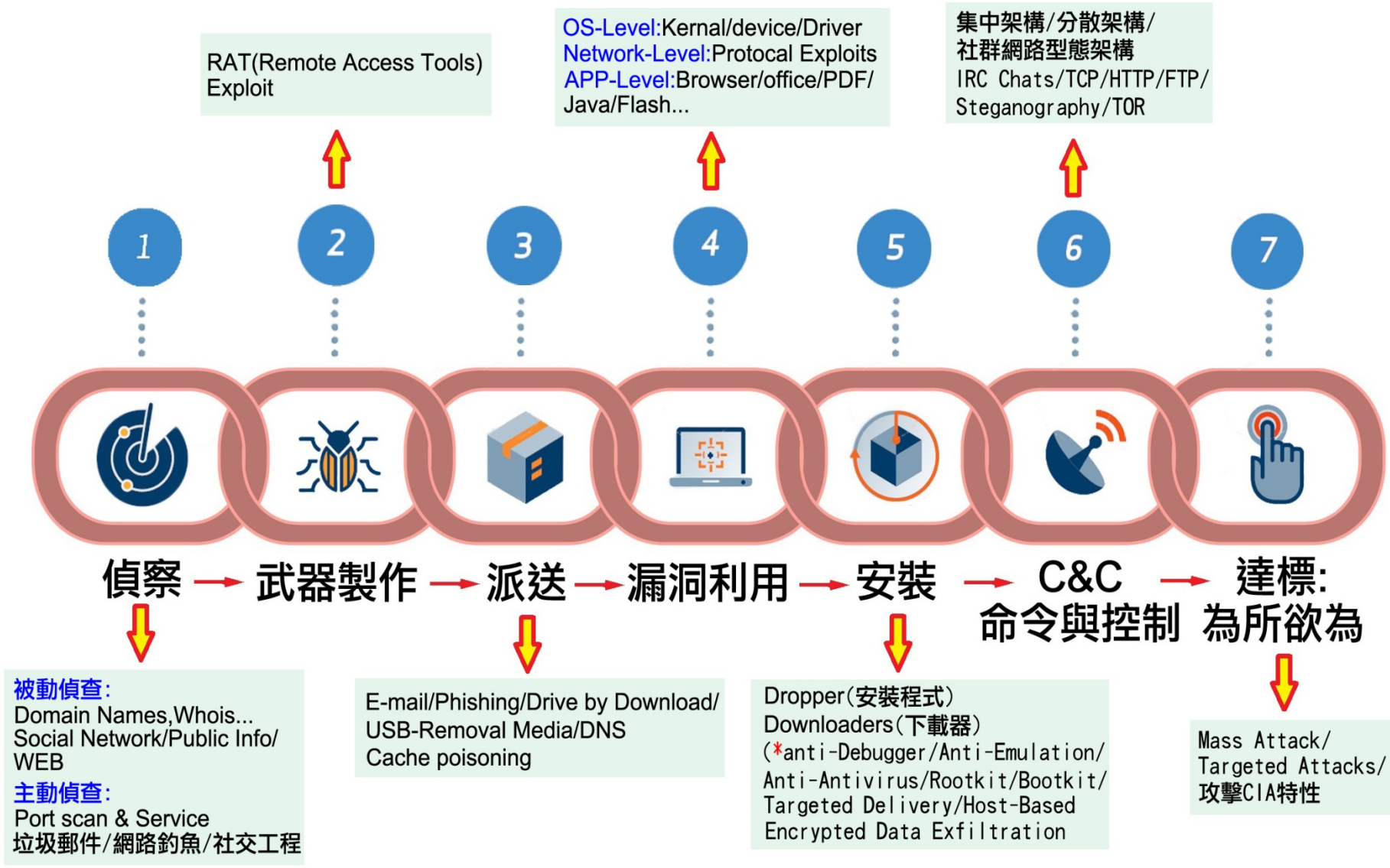
時間軸：數小時/數個月 | 數秒鐘 | 數個月至數年



準備階段 | 入侵階段 | 控制及採取行動階段

對應網路攻擊鏈(Cyber Kill Chain)框架-攻擊者常用的攻擊技術(Technical Aspects)

保安資訊 SAVETIME INFORMATION SECURITY



對應網路攻擊鏈(Cyber Kill Chain)框架-產業標準的建議防護

保安資訊 SAVETIME INFORMATION SECURITY

Phase	Detect (偵測)	Deny (避免)	Disrupt (阻止)	Degrade (降級)	Deceive (誘騙)	Contain (災情控管)
Reconnaissance (偵查)	Web Analytics	Firewall ACL				Firewall ACL
Weaponization (武器化)	NDIS	NIPS				
Delivery (傳遞)	Vigilant user(Security Awareness)	Proxy Filter	Inline AV	Queuing		APP-Aware Firewall
Exploitation (漏洞利用)	HIDS	Patch	DEP			Inter-Zone NIPS
Installation (安裝)	HIDS	'Chroot' Jail	AV			EPP
Command and Control (命令與控制)	NDIS	Firewall ACL	NIPS	Tarpit	DNS Redirect	Trust zones
Action on Targets(達標)	Audit Logs	Outbound ACL	DLP	Quality of service	Honeypot	Trust zones

對應網路攻擊鏈(Cyber Kill Chain)框架-Symantec 提供業界最完善的防護保護方案

保安資訊 SAVETIME INFORMATION SECURITY

Phase	Detect(偵測)	Deny(避免) or Contain(災情限制/控制)	Disrupt(阻止)、Eradicate(根除) or Deceive(誘騙)	Recover(恢復)
Reconnaissance (偵查)	DeepSight Threat Intelligence、MSS(Managed Security Services) 、CSS(Control Compliance Suite)、SMG(*DHA Protect)	CSS, DCS(Data center Security)	N/A	N/A
Weaponization (武器化)	DeepSight™ Adversary Intelligence	CSS、Altiris ITMS (Symantec™ IT Management Suite)	SMG(Decoy Account)、Symantec.Security.cloud(email/web)	N/A
Delivery (傳遞)	MSS、DeepSight™ Intelligence 、$Blackfin(user training,phishing tests)	ATP、Deepsight Threat Intellgence	SEP(*AV(Sonar/Insight)/*HIPS)	SEP(*Power Eraser)、Veritas
Exploitation (漏洞利用)	SEP(*HIPS/*HI)、DCS、MSS	SEP(*FW)、DCS、ATP、DeepSight™ Intelligence	SEP(AV)、ATP、DCS	Veritas
Installation (安裝)	SEP、ATP、DCS	SEP、Moblity Suite、Authentication Manager、VIP,Managed PKI	SEP(*AV/*HIPS/*HI)、ATP(Sandbox & Correlation)、DCS(Sandbox/完全白名單/帳戶權限限縮)	Incident Response Retainer Services
Command and Control (命令與控制)	SWG、ATP、MSS、DeepSight™ Intelligence 、$BlueCoat	DeepSight™ Intelligence、DLP、ATP	DeepSight™ Intelligence	Incident Response Retainer Services
Action on Targets(達標)	MSS、DLP、DeepSight™ Intelligence	DLP (Symantec Data Loss Prevention)	DLP、ATP	Incident Response Retainer Services

對應網路攻擊鏈(CKC):
Symantec產品的防護/Hardening Tips

防護產品: SMG
(Symantec Message Gateways)

保安資訊 SAVETIME INFORMATION SECURITY

郵件及訊息閘道安全

Symantec Messaging Gateway

不只是反垃圾郵件全球第一品牌

SMG集六大安全功能於一身:

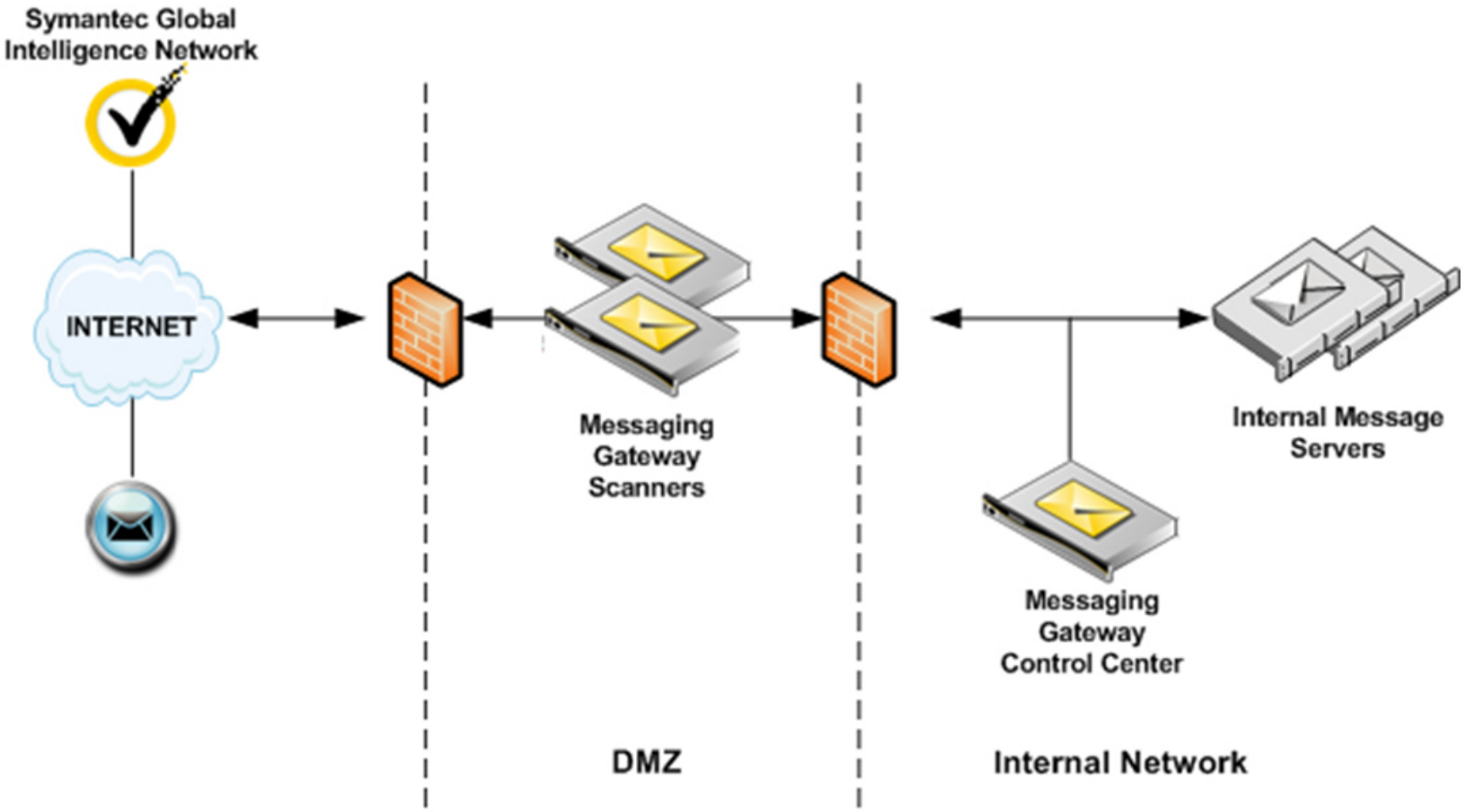
1.防垃圾郵件 2.防惡意程式 3.內容過濾

4.資料遺失預防 5.即時通訊安全 6.郵件加密

Hyper-V or vmware

實體專用硬體主機與VM/Hyper-V三平台版本同時推出

SMG:部署位於閘道第一關



A closer look at Symantec Messaging Gateway

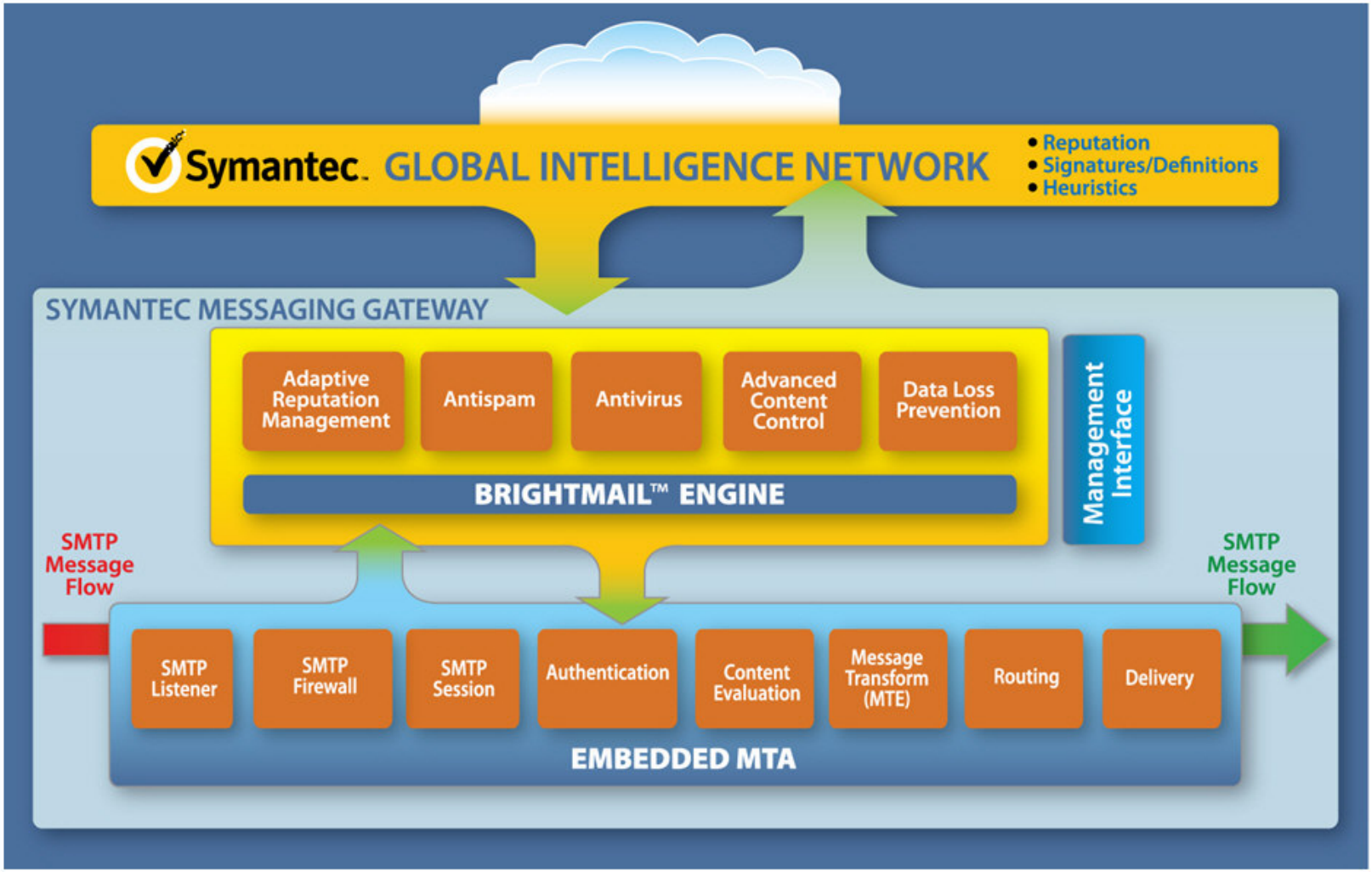
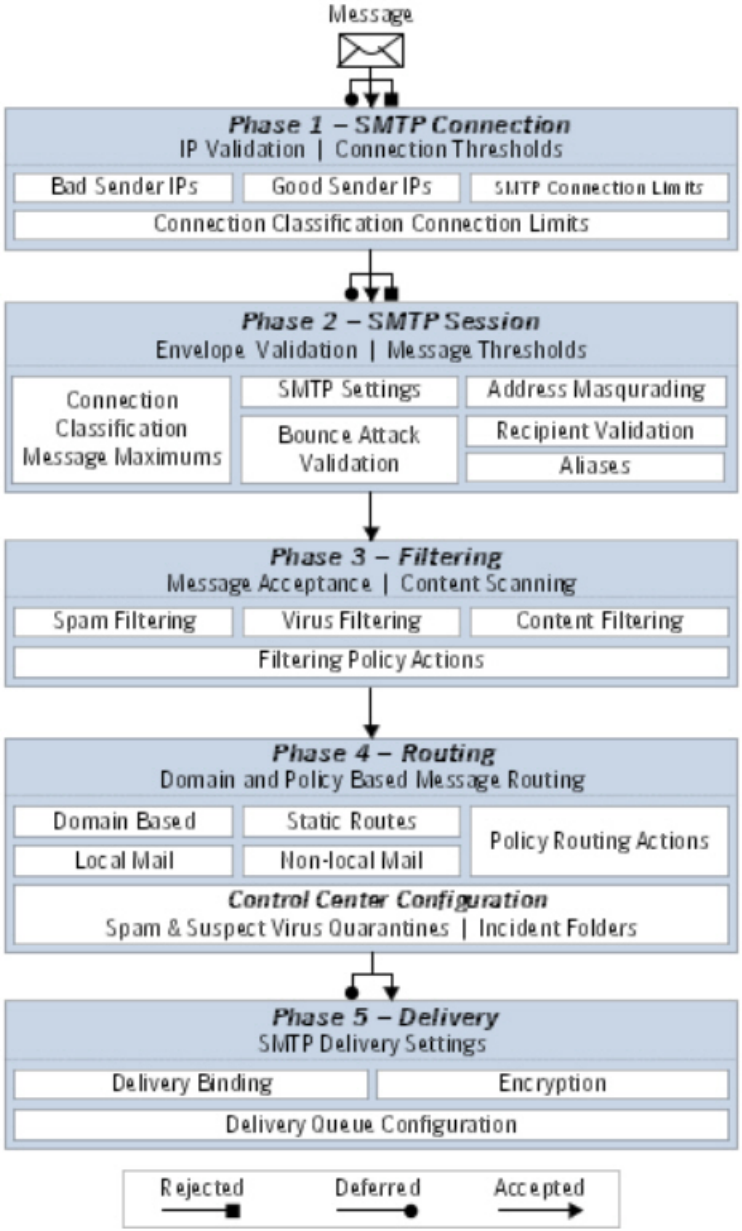


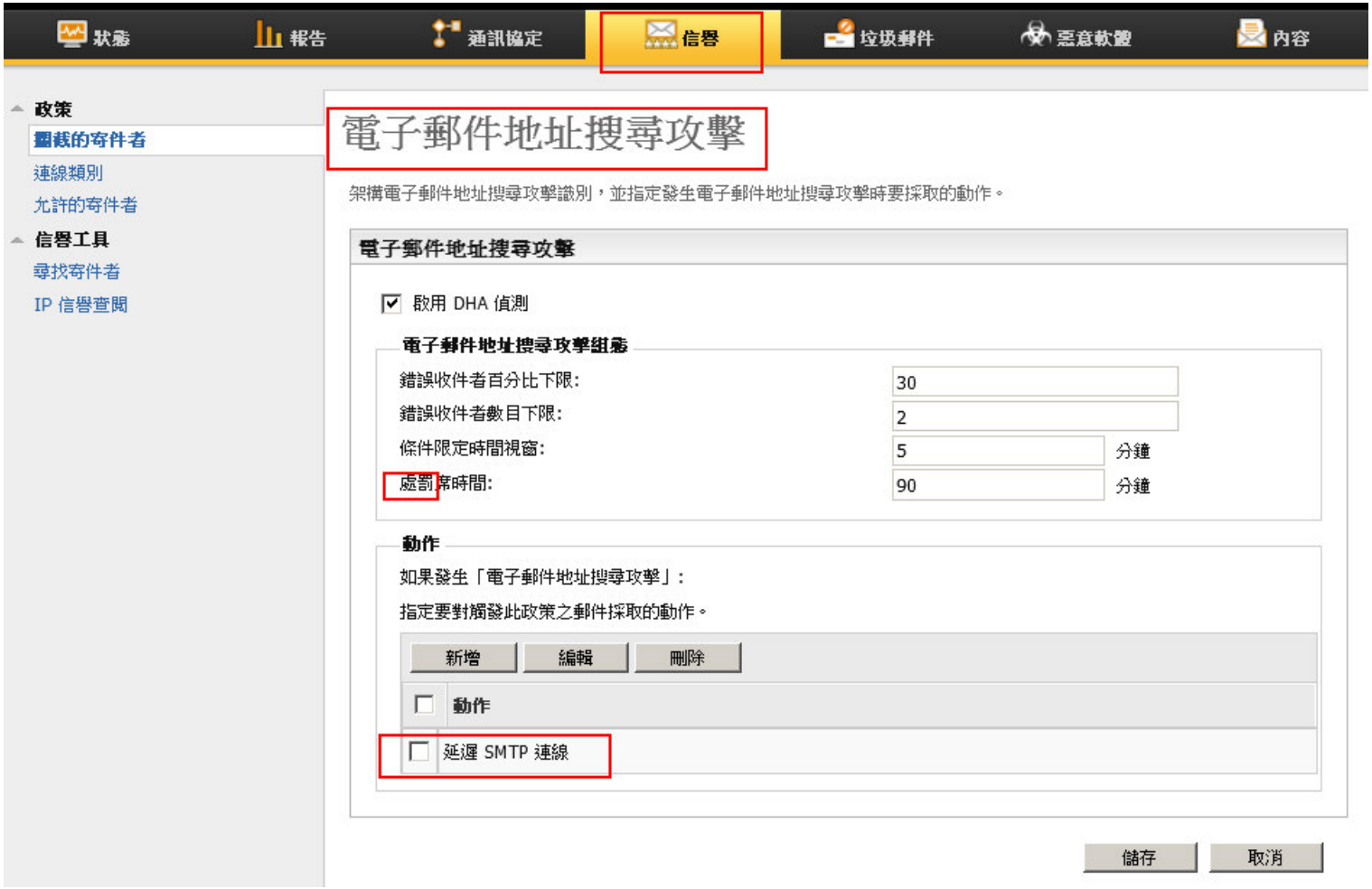
Figure: Inbound Message Flow



偵察

SMG:網路層防火牆->阻止電子郵件搜尋攻擊

保安資訊 SAVETIME INFORMATION SECURITY



內容過濾:不安全的執行檔附件 ->多重處置

SMG:系統預設的可執行檔類型，可自行再增減

保安資訊 SAVETIME INFORMATION SECURITY

派送

- 附件類型
- 真實檔案類型 是 ELF Executable
- 真實檔案類型 是 MS-DOS Batch File
- 真實檔案類型 是 MSDOS Device Driver
- 真實檔案類型 是 MSDOS/Windows Program
- 真實檔案類型 是 PC (.COM)
- 真實檔案類型 是 Unix Executable (3B20)
- 真實檔案類型 是 Unix Executable (Basic-16)
- 真實檔案類型 是 Unix Executable (Bell 5.0)
- 真實檔案類型 是 Unix Executable (iAPX 286)

- MIME-類型 開頭是 application/bat
- MIME-類型 開頭是 application/com
- MIME-類型 開頭是 application/exe
- MIME-類型 開頭是 application/hta
- MIME-類型 開頭是 application/javascript
- MIME-類型 開頭是 application/x-bat
- MIME-類型 開頭是 application/x-com
- MIME-類型 開頭是 application/x-download
- MIME-類型 開頭是 application/x-exe
- MIME-類型 開頭是 application/x-helpfile
- MIME-類型 開頭是 application/x-javascript

- 副檔名 是 ade
- 副檔名 是 adp
- 副檔名 是 app
- 副檔名 是 bas
- 副檔名 是 bat
- 副檔名 是 bin
- 副檔名 是 chm
- 副檔名 是 class
- 副檔名 是 cmd
- 是 com
- 副檔名 是 ins
- 副檔名 是 isp
- 副檔名 是 js
- 副檔名 是 jse
- 副檔名 是 lnk
- 副檔名 是 mda
- 副檔名 是 mdb
- 副檔名 是 mde
- 副檔名 是 mdt
- 副檔名 是 mdw
- 副檔名 是 mdz

- 副檔名 是 com
- 副檔名 是 cpl
- 副檔名 是 crt
- 副檔名 是 dll
- 副檔名 是 drv
- 副檔名 是 exe
- 副檔名 是 fxp
- 副檔名 是 hlp
- 副檔名 是 hta
- 副檔名 是 inf
- 副檔名 是 ink

- 副檔名 是 scr
- 副檔名 是 sct
- 副檔名 是 shb
- 副檔名 是 shs
- 副檔名 是 sys
- 副檔名 是 url
- 副檔名 是 vb
- 副檔名 是 vbe
- 副檔名 是 vbs
- 副檔名 是 vxd
- 副檔名 是 wsc

- 副檔名 是 msc
- 副檔名 是 msi
- 副檔名 是 msp
- 副檔名 是 mst
- 副檔名 是 nlm
- 副檔名 是 ops
- 副檔名 是 ovl
- 副檔名 是 pcd
- 副檔名 是 pif
- 副檔名 是 prf
- 副檔名 是 prg

SMG: Disarm
(解除Office/PDF 檔案的物件)

派送

保安資訊 SAVETIME INFORMATION SECURITY

New: Gateway:
Disarm for Symantec Messaging Gateway

- Disarm removes all active content and reconstructs a clean version
- Clean attachment is delivered in real-time
- User is **never exposed** to the attack

Blocked

98%

of Zero Day Exploits in 2013

Works with

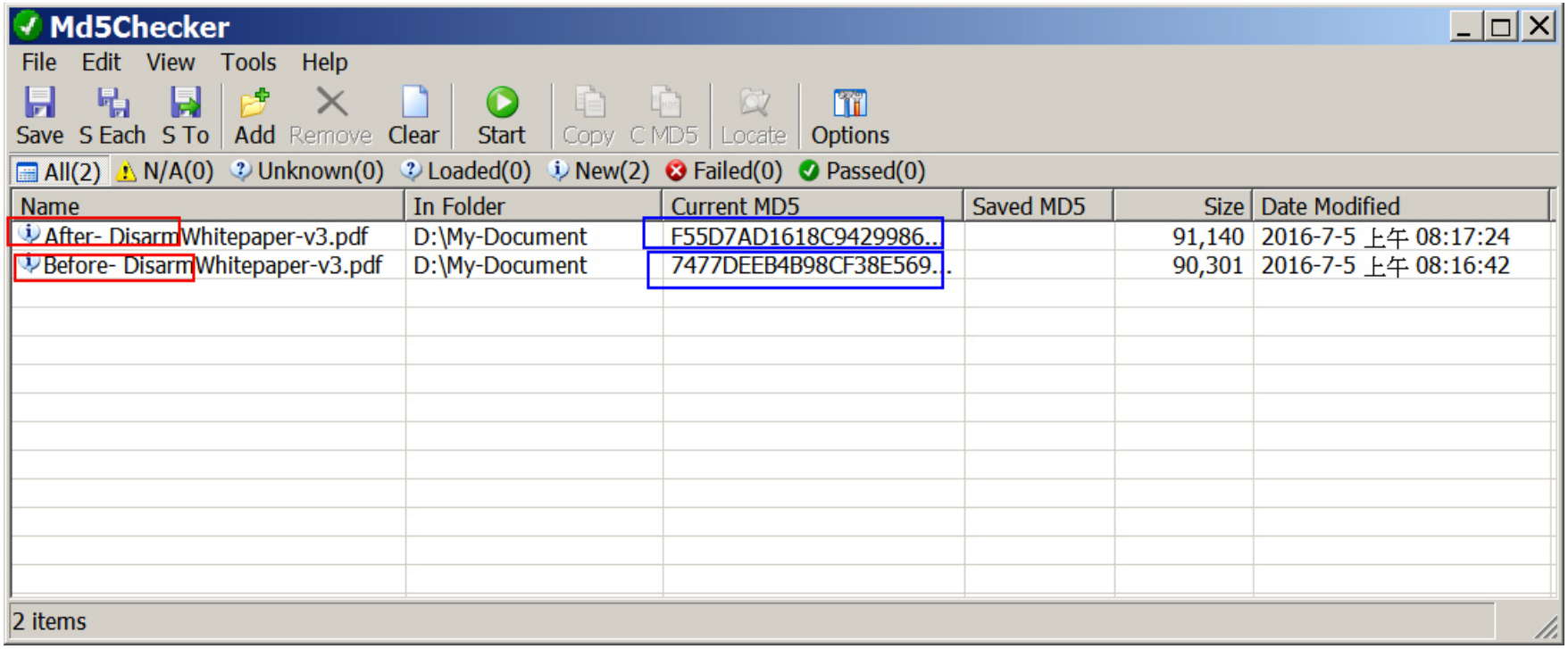
Attachments

SMG:Disarm, 支援的檔案類型&物件

SMG: Disarm政策,先保留一份稽核再解除物件

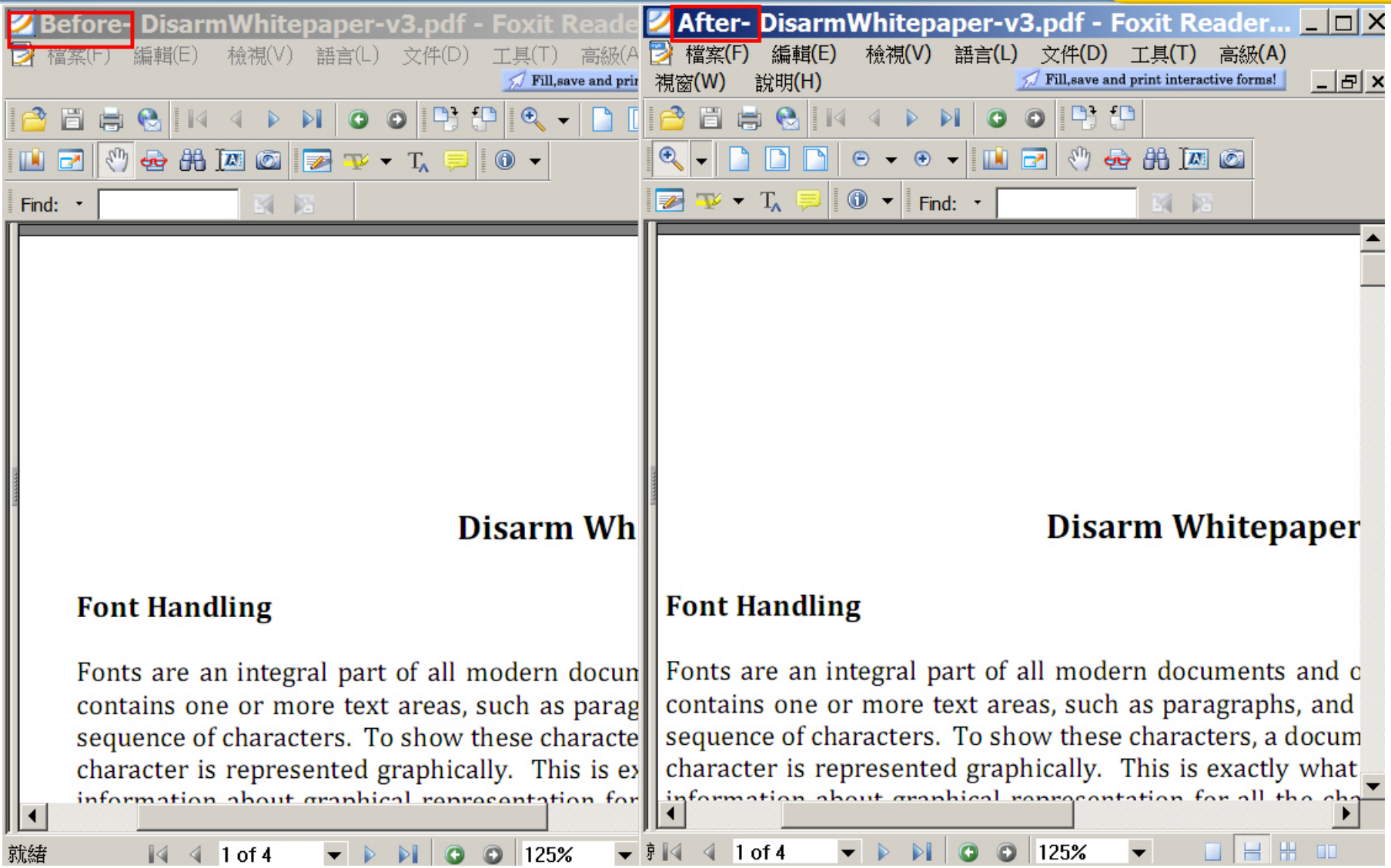
SMG:檔案經 Disarm 後,檔案已被修改

保安資訊 SAVETIME INFORMATION SECURITY



SMG:檔案經Disarm後,不影響"可讀性"

保安資訊 SAVETIME INFORMATION SECURITY



SMG:連線類別,網路層流量管控

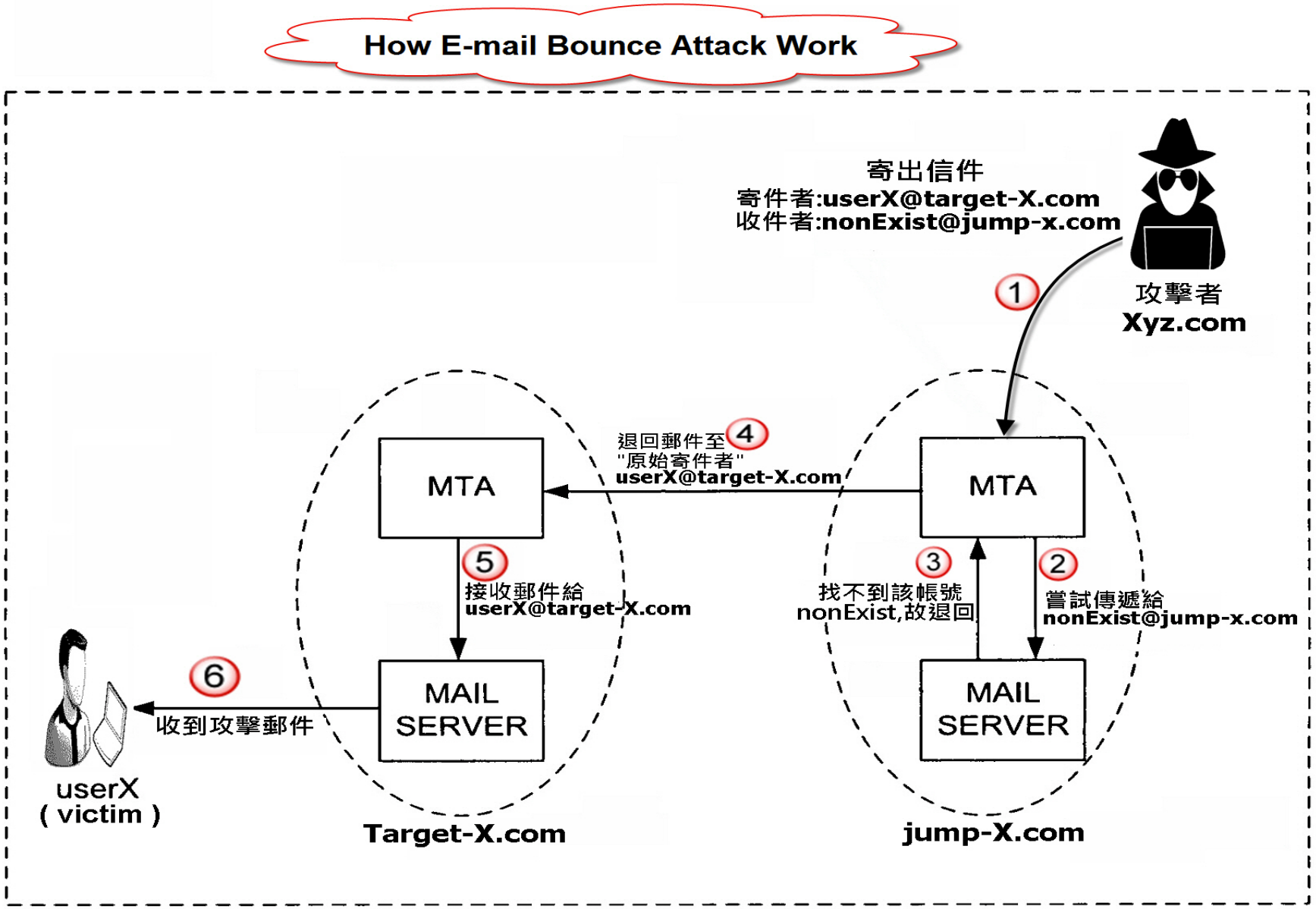
SMG:網路層流量管控,基於IP連線歷史資料智慧分析

保安資訊 SAVETIME INFORMATION SECURITY

Symantec Messaging Gateway does not take any action based on Connection Classification until the appliance has recorded enough data to make accurate predictions. Immediately after the initial installation of a Scanner, Connection Classification is in learning mode. **Learning mode ends when 50,000 messages** are received and the statistics gathered from them have been added to the database.

SMG:防禦電子郵件退回攻擊

電子郵件退回攻擊的原理



產品:SEP(SymantecEndpoint Protection)應用程式控制,預設的Policy可阻擋常見的惡意程式非經授權存取

保安資訊 SAVETIME INFORMATION SECURITY

0-Harden-Default-應用程式及裝置控制政策

應用程式和裝置控制
政策

概述
應用程式控制
裝置控制

應用程式控制

應用程式控制規則集

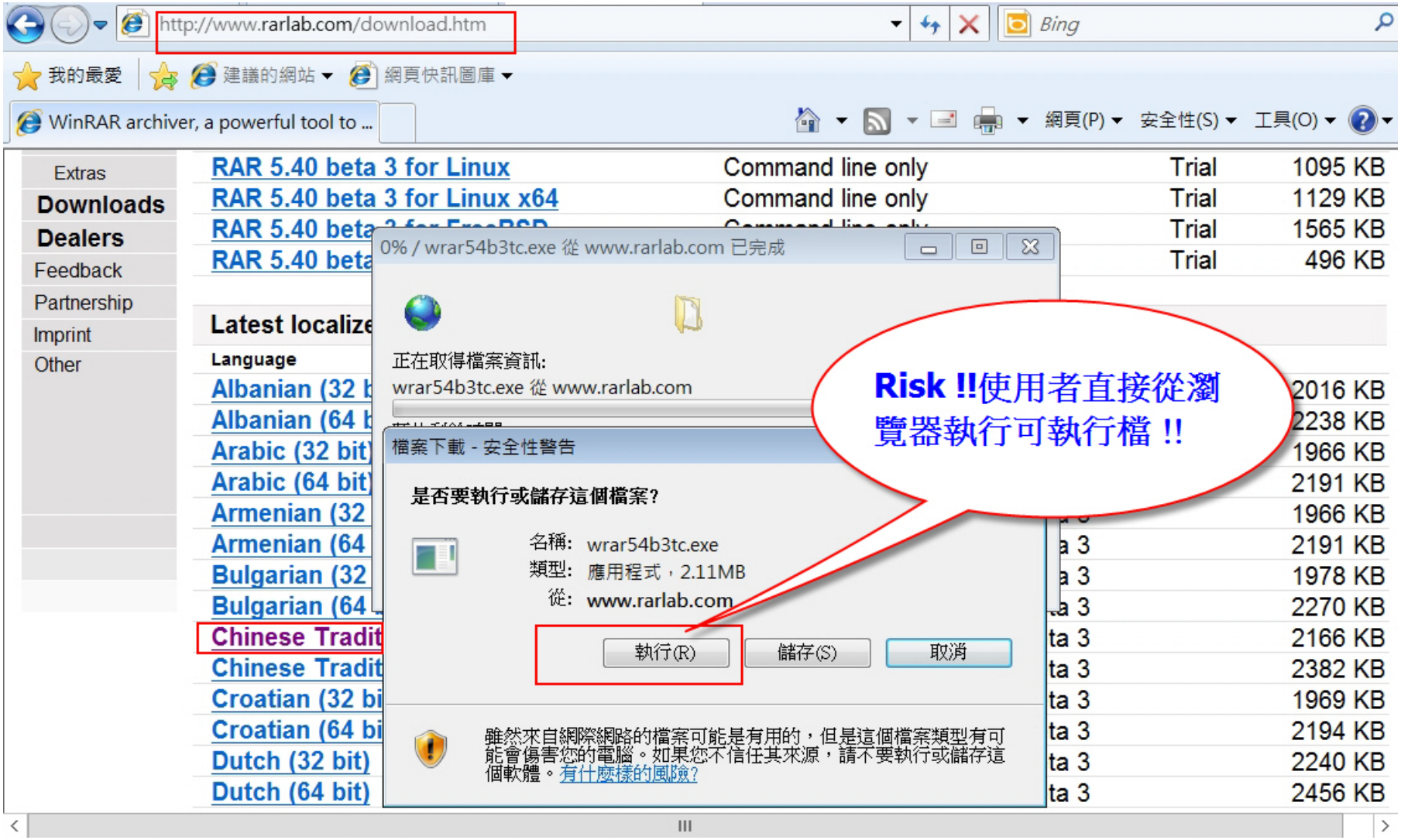
「應用程式控制」會限制應用程式可執行的動作以及可使用的系統資源。「應用程式控制」具有多項功用，包括防止惡意軟體劫取應用程式、防範不慎移除貴公司的機密資料，以及限制可執行的應用程式。

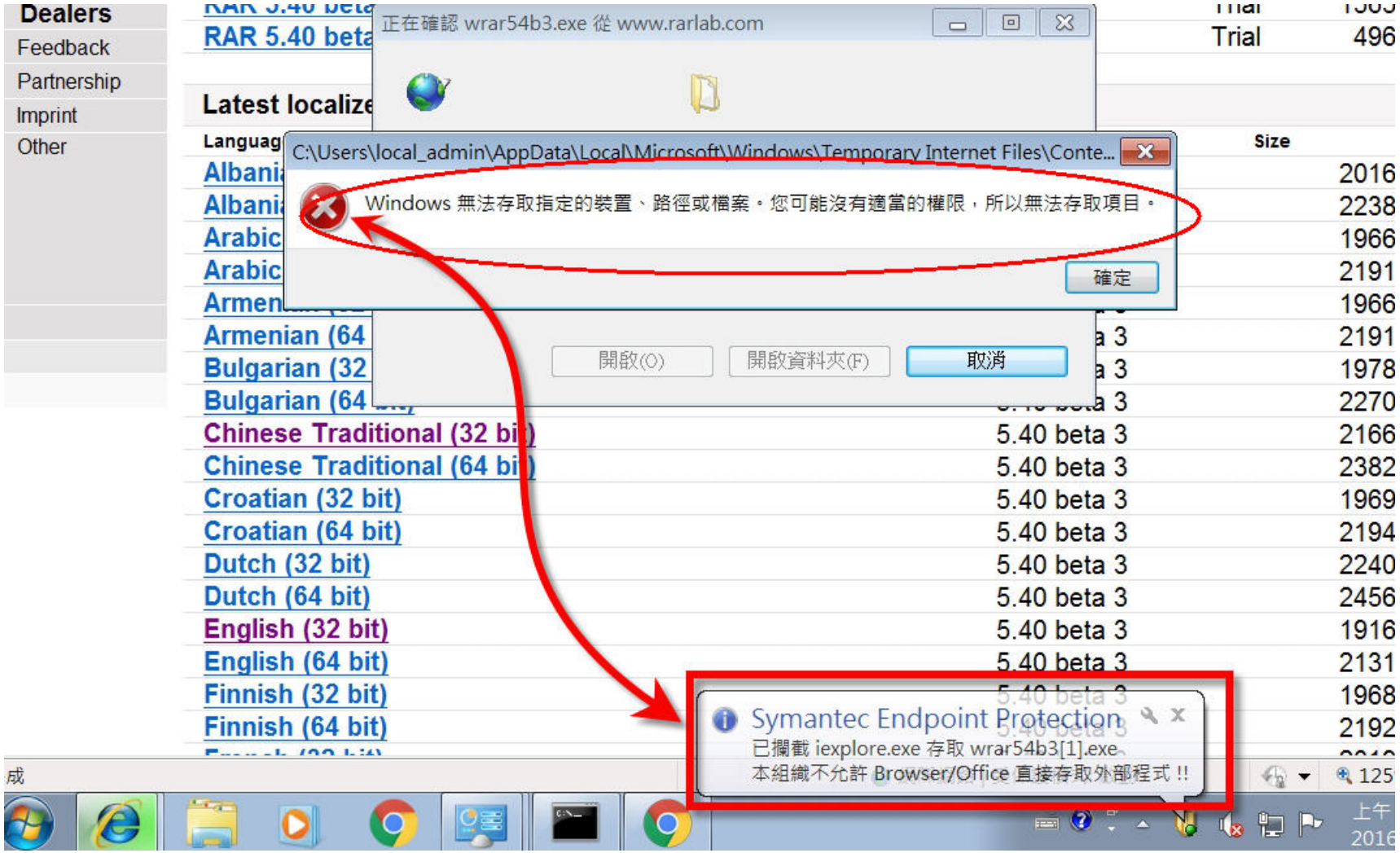
只有進階管理員可建立「應用程式控制」規則集。

已啟用	規則集	測試/正式
☑	防止用戶端改IP-Win7-2008-Vista 的副本	正式
☐	攔阻應用程式執行 [AC1]	正式
☐	攔截從卸除式磁碟機執行程式 [AC2]	正式
☐	將全部卸除式磁碟機設定為唯讀 [AC3]	正式
☐	[AC4-1.1] 攔截向 USB 磁碟機寫入內容	正式
☐	[AC5-1.1] 記錄向 USB 磁碟機寫入的內容	正式
☐	攔截對主機檔案的修改	正式
☑	攔截存取程序檔	測試 (只記錄)
☐	停止軟體安裝程式 [AC8]	正式
☑	攔截存取 Autorun.inf [AC9]	正式
☐	攔截密碼重設工具 [AC10]	正式
☐	攔截檔案共用 [AC11]	正式
☐	防止變更 Windows shell 載入點 (HIPS) [AC12]	正式
☑	防止使用瀏覽器和 Office 產品變更系統 (HIPS) [AC13]	測試 (只記錄)
☐	防止修改系統檔案 (HIPS) [AC14]	測試 (只記錄)
☑	防止註冊新的瀏覽器協助程式物件 (HIPS) [AC15]	正式
☑	防止註冊新的工具列 (HIPS) [AC16]	正式
☐	防止容易遭到攻擊的 Windows 程序撰寫程式碼 [AC17]	正式
☐	防止 Windows 服務使用 UNC 路徑 [AC-23]	正式
☐	攔截對 lnk 和 pif 檔案的存取 [AC-24]	正式
☐	攔截應用程式用盡資源回收筒 [AC-25]	正式

新增... 編輯... 刪除 上移 下移

確定 取消 說明


http://www.rarlab.com/download.htm
Bing
我的最愛
建議的網站
網頁快訊圖庫
WinRAR archiver, a powerful tool to ...
網頁(P)
安全性(S)
工具(O)
Extras
Downloads
Dealers
Feedback
Partnership
Imprint
Other
RAR 5.40 beta 3 for Linux
Command line only
Trial
1095 KB
RAR 5.40 beta 3 for Linux x64
Command line only
Trial
1129 KB
Trial
1565 KB
Trial
496 KB
Latest localize
Language
Albanian (32 b
Albanian (64 b
Arabic (32 bit)
Arabic (64 bit)
Armenian (32
Armenian (64
Bulgarian (32
Bulgarian (64
Chinese Tradit
Chinese Tradit
Croatian (32 bi
Croatian (64 bi
Dutch (32 bit)
Dutch (64 bit)
2016 KB
2238 KB
1966 KB
2191 KB
1966 KB
2191 KB
1978 KB
2270 KB
2166 KB
2382 KB
1969 KB
2194 KB
2240 KB
2456 KB
0% / wrar54b3tc.exe 從 www.rarlab.com 已完成
正在取得檔案資訊:
wrar54b3tc.exe 從 www.rarlab.com
檔案下載 - 安全性警告
是否要執行或儲存這個檔案?
名稱: wrar54b3tc.exe
類型: 應用程式，2.11MB
從: www.rarlab.com
執行(R)
儲存(S)
取消
雖然來自網際網路的檔案可能是有用的，但是這個檔案類型有可能會傷害您的電腦。如果您不信任其來源，請不要執行或儲存這個軟體。有什麼樣的風險?
Risk !!使用者直接從瀏覽器執行可執行檔 !!


Dealers
Feedback
Partnership
Imprint
Other
RAR 5.40 beta
Trial 496
Latest localize
Languag
Size
Albani 2016
Albani 2238
Arabic 1966
Arabic 2191
Armen 1966
Armenian (64 2191
Bulgarian (32 1978
Bulgarian (64 2270
Chinese Traditional (32 bi) 5.40 beta 3 2166
Chinese Traditional (64 bi) 5.40 beta 3 2382
Croatian (32 bit) 5.40 beta 3 1969
Croatian (64 bit) 5.40 beta 3 2194
Dutch (32 bit) 5.40 beta 3 2240
Dutch (64 bit) 5.40 beta 3 2456
English (32 bit) 5.40 beta 3 1916
English (64 bit) 5.40 beta 3 2131
Finnish (32 bit) 1968
Finnish (64 bit) 2192
正在確認 wrar54b3.exe 從 www.rarlab.com
C:\Users\local_admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Conte...
Windows 無法存取指定的裝置、路徑或檔案。您可能沒有適當的權限，所以無法存取項目。
確定
開啟(O)
開啟資料夾(F)
取消
Symantec Endpoint Protection
已攔截 iexplore.exe 存取 wrar54b3[1].exe
本組織不允許 Browser/Office 直接存取外部程式 !!

老舊應用程式vendor 已不再更新, 安全堪虞

漏洞利用

保安資訊 SAVETIME INFORMATION SECURITY

Google Chrome 已停止支援 Windows XP 和 Windows Vista，因此這部電腦不會再收到 Google Chrome 更新。 瞭解詳情

Updates to Chrome platform supp

Tuesday, November 10, 2015

Earlier this year, we announced that Google Chr
Windows XP through the remainder of 2015. A
users on older, unsupported platforms such as
secure operating system. Such older platforms
and have a greater potential to be infected by viruses and malware.

Today, we're announcing the end of Chrome's support for Windows XP, as well as Windows Vista, and Mac OS X 10.6, 10.7, and 10.8, since these platforms are no longer actively supported by Microsoft and Apple. Starting April 2016, Chrome will continue to function on these platforms but will no longer receive updates and security fixes.

If you are still on one of these unsupported platforms, we encourage you to move to a newer operating system to ensure that you continue to receive the latest Chrome versions and features.

Posted by Marc Pawliger, Director of Engineering and Early Notifier

關於

Google Chrome
簡單、快速又安全的網路瀏覽器

前往 Chrome 說明頁面 回報問題

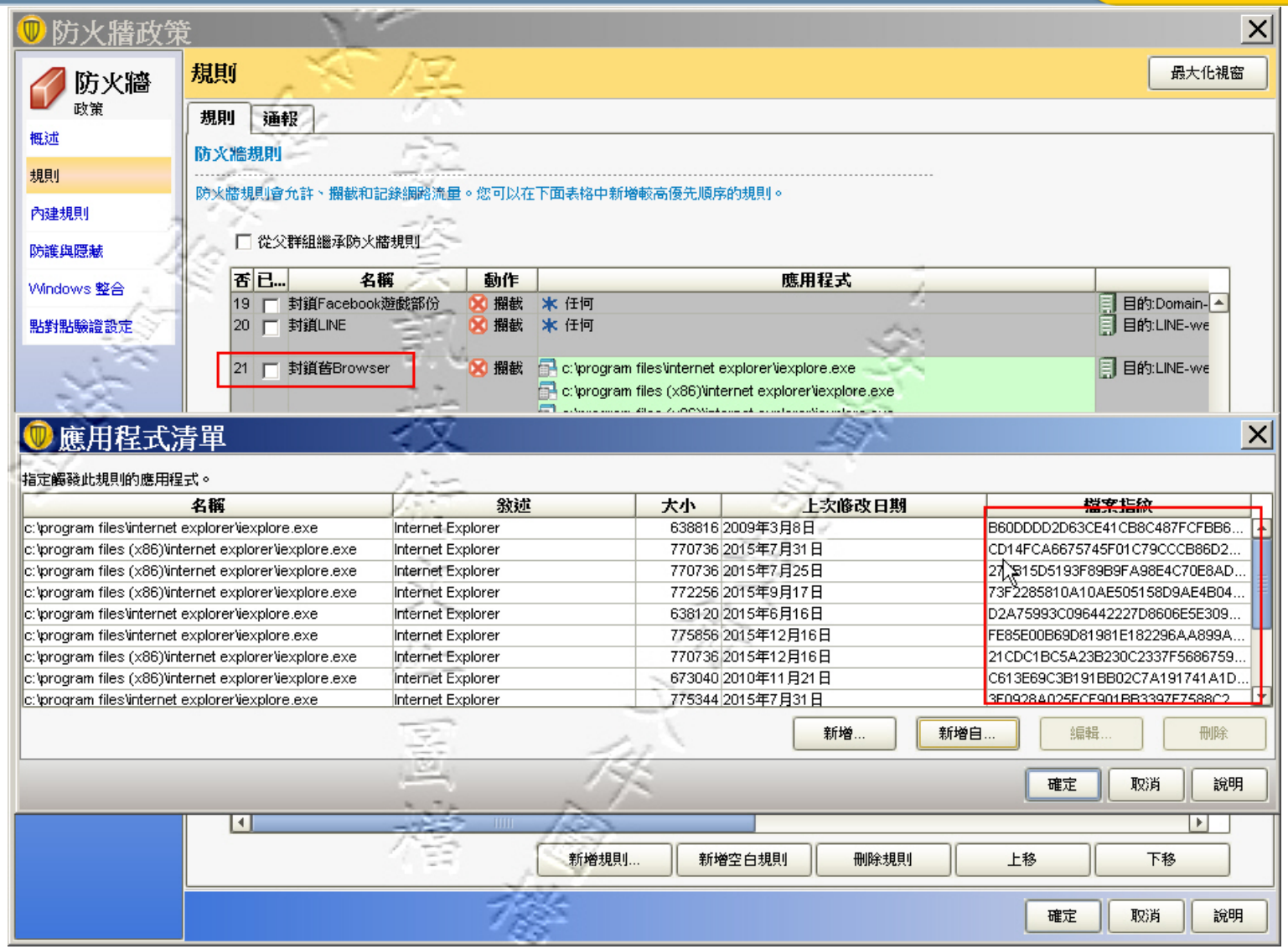
版本 49.0.2623.112 m

Google Chrome 已停止支援 Windows XP 和 Windows Vista，因此這部電腦不會再收到 Google Chrome 更

漏洞利用

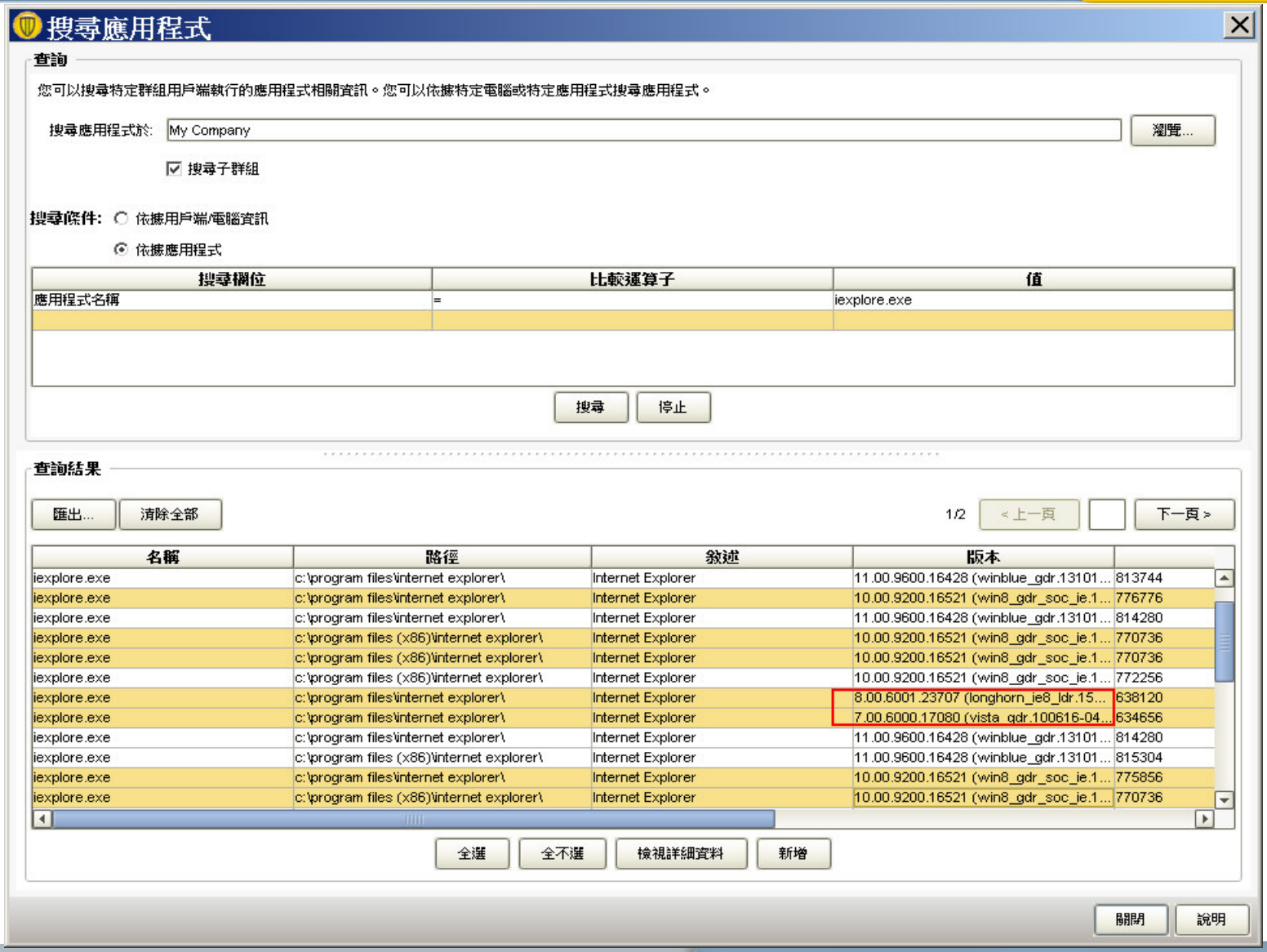
SEP:防火牆可封鎖老舊應用程式連外,此處IE為例,其他Chrome,Firefox,flash,java等亦同!

保安資訊 SAVETIME INFORMATION SECURITY

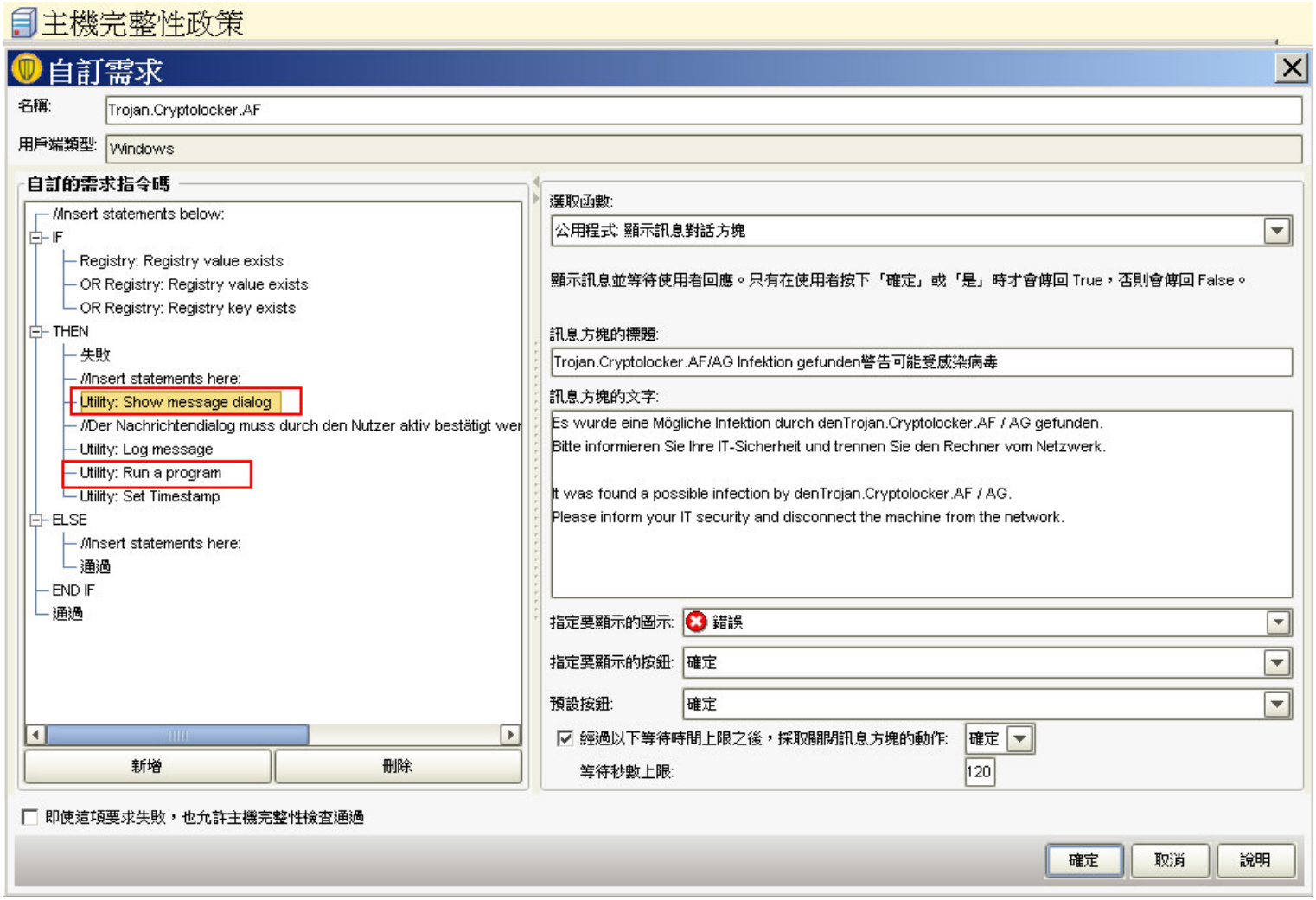


SEP:應用程式資料收集,方便管理者制定政策

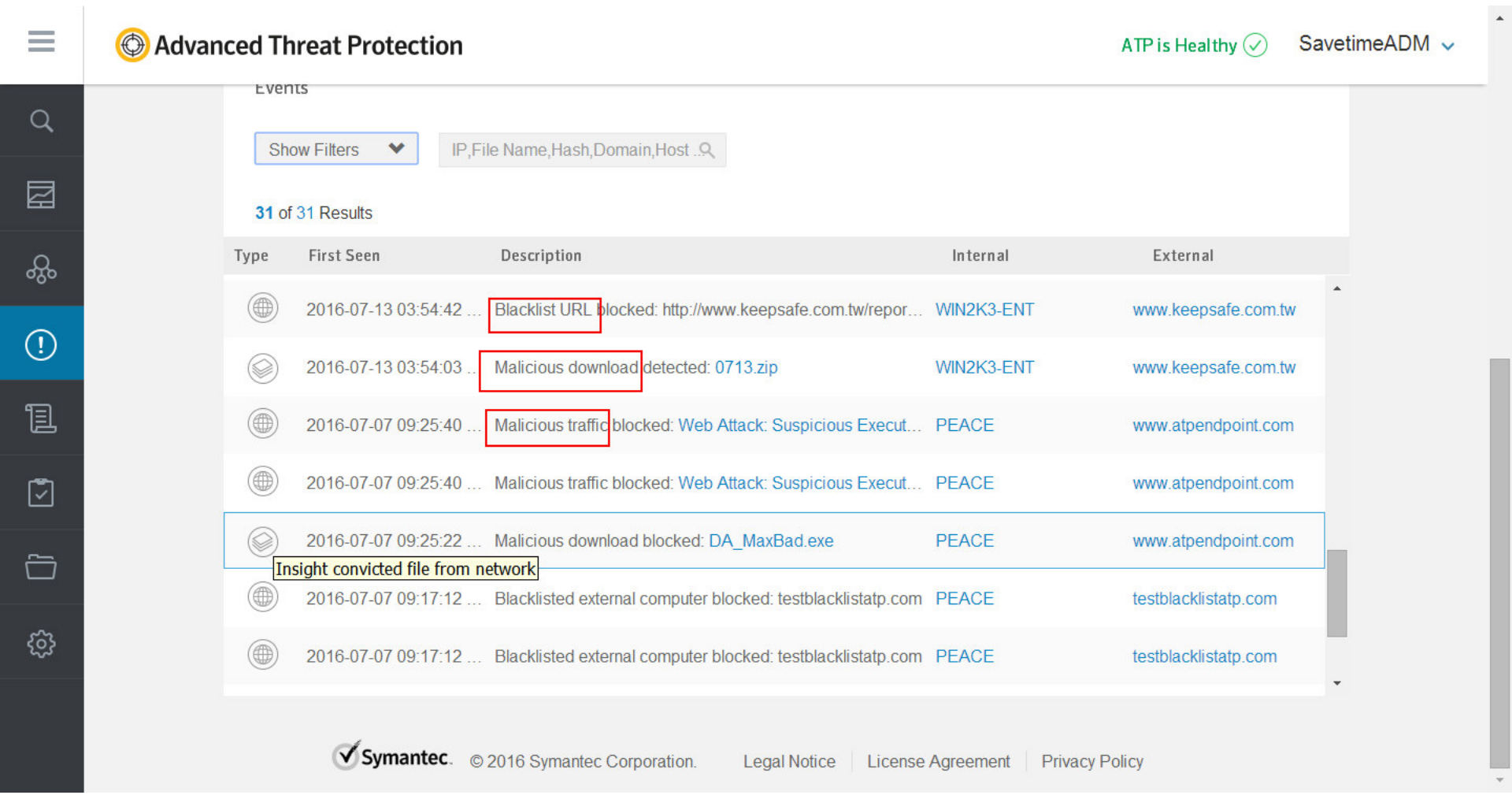
保安資訊 SAVETIME INFORMATION SECURITY



SEP:主機完整性檢查->事後補救&災情控制



產品:ATP(Advanced Threat Protection,Network+Endpoint)



ATP(已整合Endpoint),可直接於ATP介面隔離有風險的用戶端電腦

保安資訊 SAVETIME INFORMATION SECURITY

Advanced Threat Protection

ATP is Healthy

Savet

Endpoint: 192.168.188.5

At Risk
DISPOSITION

192.168.188.5
HOST NAME

192.168.188.5
LAST IP ADDRESS

2016-07-19 03:30:54 UTC
ATP LAST SEEN TIME

Not Available
HOST DOMAIN / WORKGROUP INFO

Not Available
MAC ADDRESS

Not Available
SEPM GROUP

Not Available
USER NAME

Not Available
OPERATING SYSTEM

Not Available
64-BIT

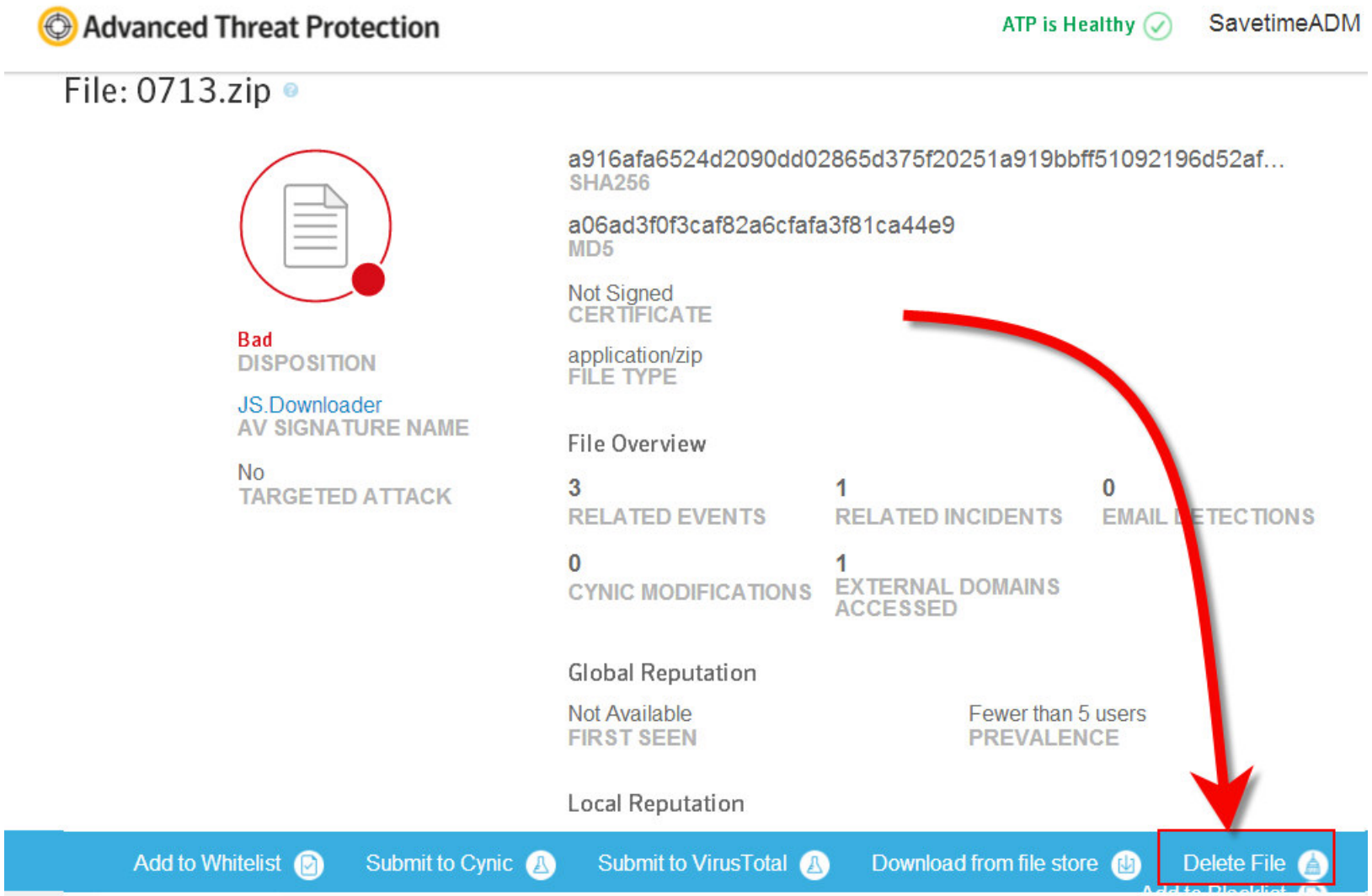
Isolate

Related Incidents

Description	Date Created	Current State	Priority
Multiple attacks have been detected targeting 192...	2016-07-19 03:30:54 UTC	Open	Low

1 Total

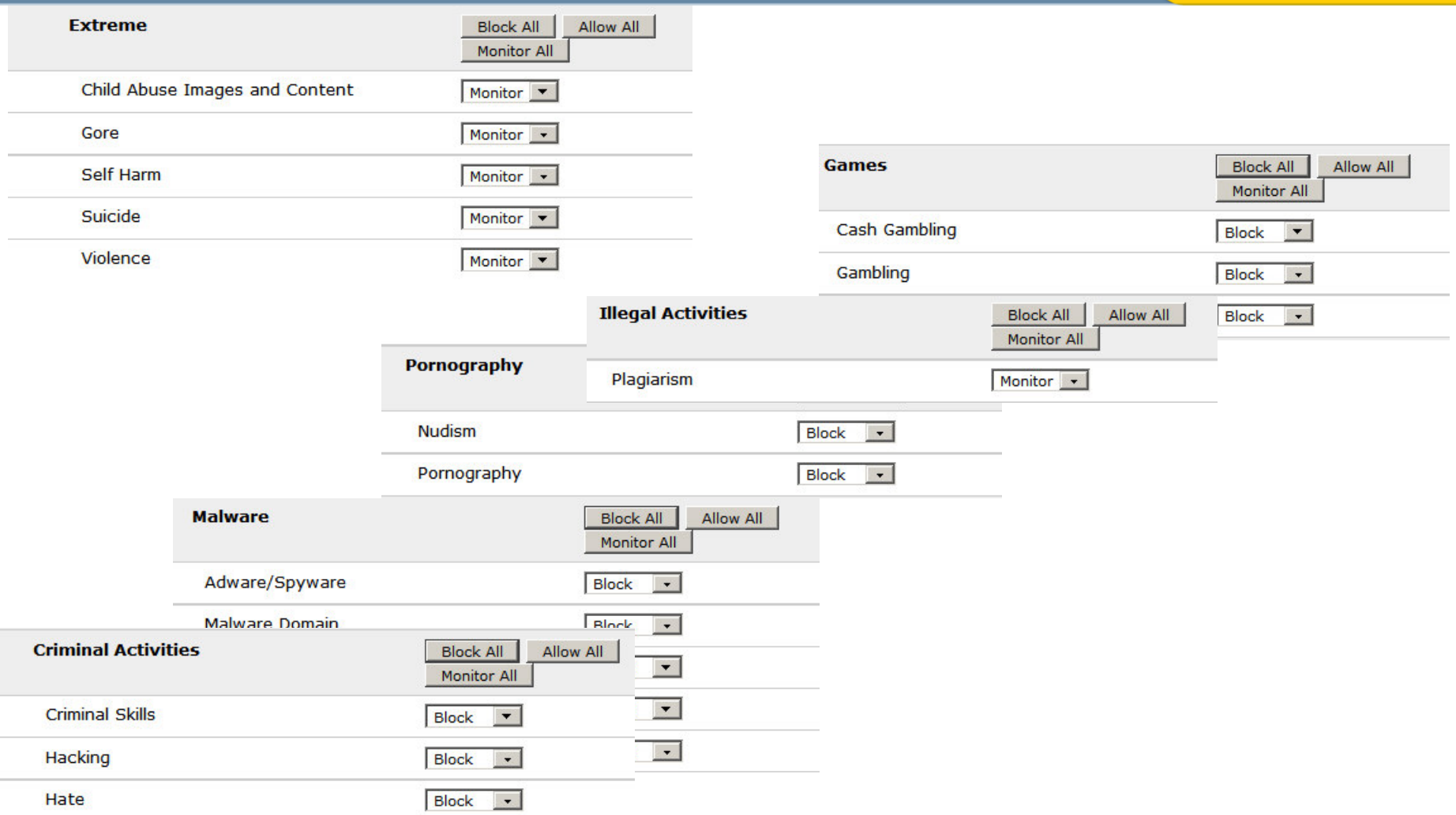
ATP(已整合Endpoint),可直接於ATP介面刪除(或黑名單化) 用戶端電腦內有害檔案



產品:SWG(Symantec Web Gateway) URL Filter阻擋

派送

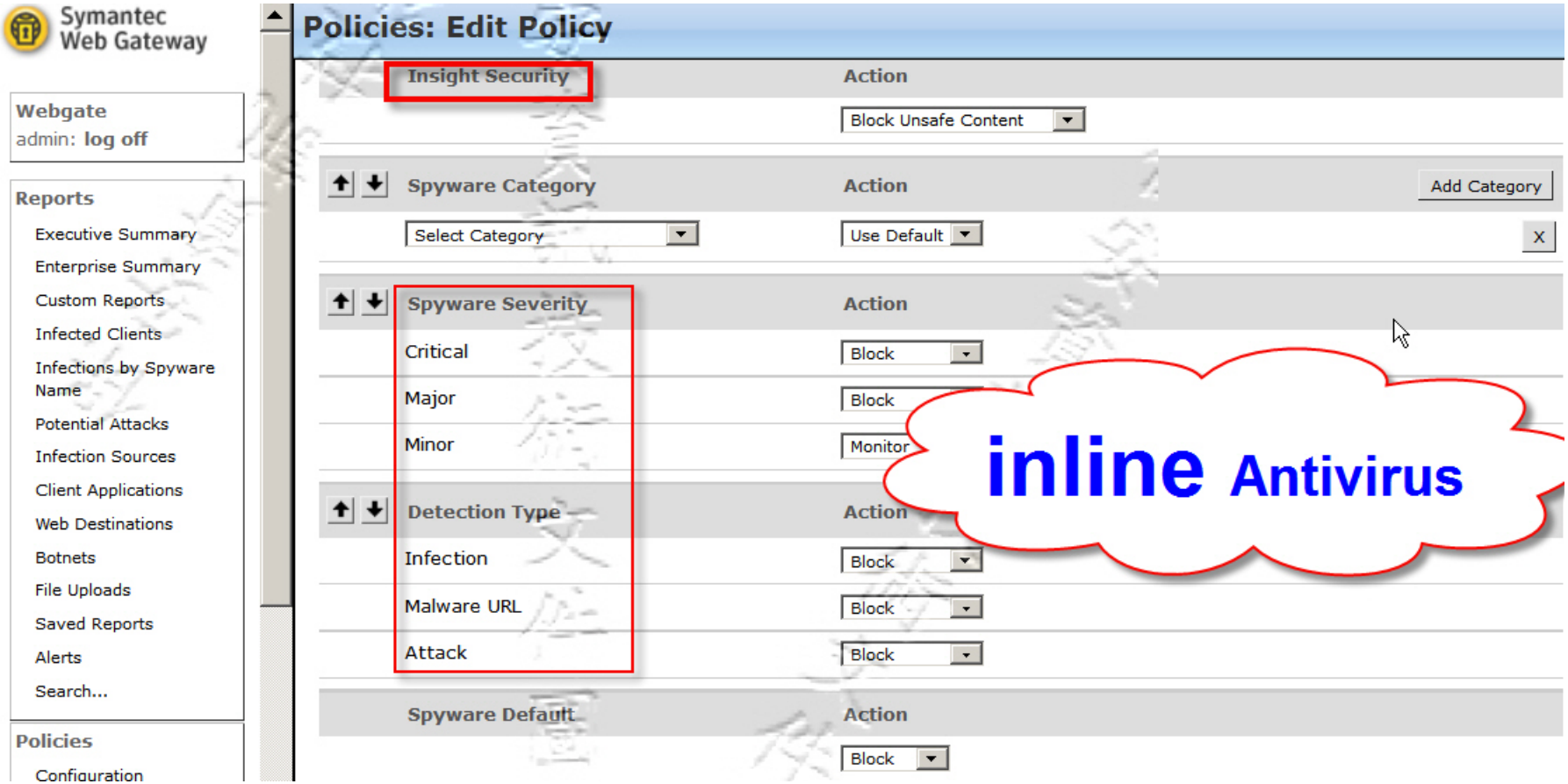
保安資訊 SAVETIME INFORMATION SECURITY



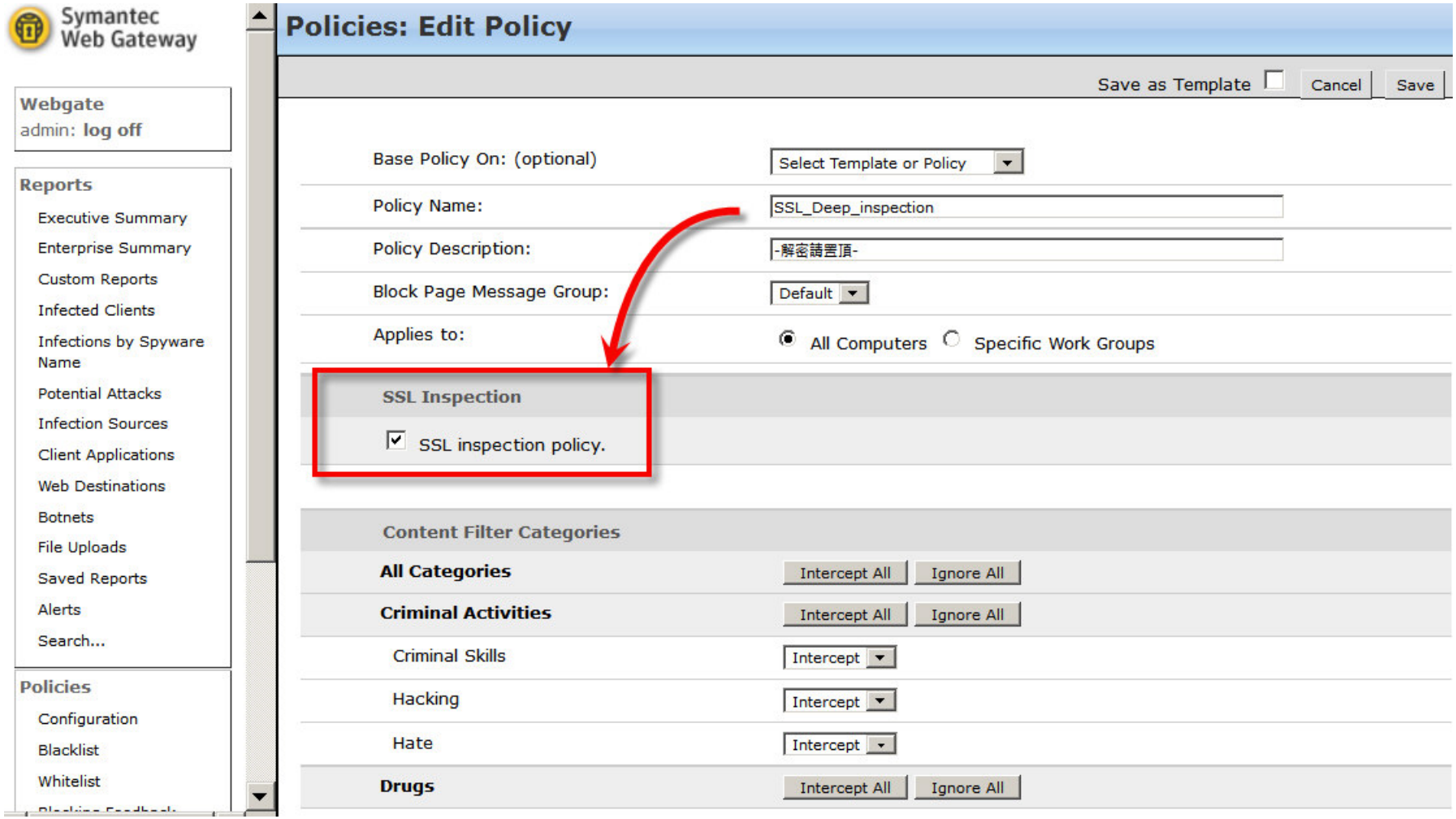
產品:SWG(Symantec Web Gateway)
Inline AV 阻擋

派送

保安資訊 SAVETIME INFORMATION SECURITY



產品:SWG(Symantec Web Gateway) SSL Inspection



產品:SWG(Symantec Web Gateway)
阻擋 malware calling home 流量

保安資訊 SAVETIME INFORMATION SECURITY

Bot IP/Hostname	Status ▲	Latest Detection	Bot Activities	Hits	C&C (Command & Control)
— 129.210.219.75	Active	01/ :39	3 Types	9,434	13 controllers
		01/ :52	Botnet Control (C&C)	5,516	67.29.139.153 68.142.205.137 72.20.40.25 72.233.2.58 74.200.243.251 76.74.254.123 76.74.255.123 98.136.92.79 208.52.165.163 216.39.57.104 216.240.187.102 216.240.187.103 216.252.126.190
		01/ :39	IP Scanning	3,914	
		01/ :26	Spyware Phone Home and Downloads	4	
— 129.210.236.83	Active	01/ :53	2 Types	3,683	6 controllers
		01/ :53	Botnet Control (C&C)	2,953	66.220.146.11 72.233.2.58 72.233.2.59 74.200.243.251 76.74.254.123 208.73.210.27
		01/ :39	IP Scanning	730	
— 129.210.239.66	Active	01/ :20	2 Types	44,225	4 controllers
		01/ :20	Botnet Control (C&C)	15,446	66.220.146.11 69.63.181.15 83.149.112.40 208.73.210.27
		01/ :15	IP Scanning	28,779	
— 129.210.129.46	Active	01/ :59	2 Types	4,028	11 controllers
		01/ :59	Botnet Control (C&C)	3,364	64.106.198.79 66.220.146.11 67.29.139.153 69.63.181.15 72.32.147.161 74.125.53.100 89.202.108.100 174.143.45.97 208.73.210.27

最後一道防線 I.
Veritas BackupExec 15:一次備份 - 多種復原選項讓作業保持簡單可靠

保安資訊 SAVETIME INFORMATION SECURITY

虛擬機器或
實體伺服器的
單程備份

儲存：
磁碟、磁帶、雲端

將整個伺服器備份至相同或不同的硬體	VM	應用程式與資料庫	檔案/資料夾	精細應用程式物件

最後一道防線II.
Veritas System Recovery 2013
數分鐘內快速復原系統

保安資訊 SAVETIME INFORMATION SECURITY