保安資訊
SAVETIME
INFORMATION SECURITY

Data Center Security
解決方案介紹說明

我們專業於資訊安全與可用性解決方案的效益最大化
滿足並超越客戶的需求

地址：台中市南屯區三和街150號
電話：0800-381500・04-23815000
www.savetime.com.tw

賽門鐵克企業市場滲透率

1. 財富前500大企業有**195**家
2. 全球前2000大企業有**697**家
3. 全球前13大銀行全都是
4. 全球前10大電信公司有**8**家
5. 全球前10大汽車製商有**7**家
6. 全球超過**1.5**億個企業用戶

關於博通賽門鐵克

- 博通賽門鐵克長期獲美國總統任命，成為美國國家安全通訊諮詢委員會(NSTAC)一員，也是目前唯四的資安廠商之一。能提供總統建言，為通訊與資訊科技重要基礎建設的安全和保護盡一份力量。
- 博通賽門鐵克也是唯一參與國際網路工程研究團隊的資安廠商(IETF:Internet Engineering Task Force)，IETF是一個開放性的國際組織，其作用在於匯集網路設計師、網路操作員、網路廠商以及研究人員共同研發改進網路的工程架構與建立起一個平穩的網路環境。例如：TLS1.3、ECH(Encrypted Client Hello)、DNS 以及HTTP……等。
- 博通賽門鐵克是開放網路安全模式框架(Open Cybersecurity Schema Framework，OCSF）專案創始成員之一，OCSF專案包含一個開放規格，以用來建立各種安全產品及服務之安全遙測的標準化資料，以及各種可支援及加速採用OCSF模式的開源工具，以協助組織更快也更有效率地偵測、調查與阻止網路攻擊。

關於我們

服務電話:
0800-381-500
+886-4-23815000

網站:
www.savetime.com.tw

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

- 保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。
- 自 1995 年起就全心全力專注在賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更熟悉用戶使用情境的優勢，能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。
- 許多顧客樂意與我們建立起長期友誼，把我們當成可信任的資安建議者、可提供良好諮商的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。

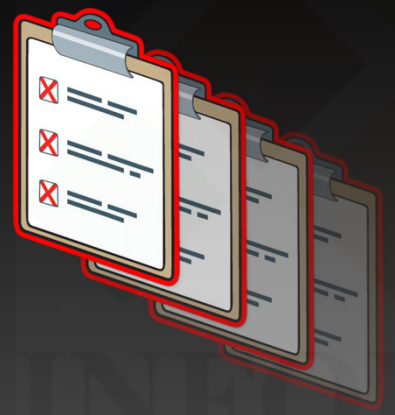
BROADCOM SOFTWARE

保安資訊 SAVETIME INFORMATION SECURITY

行為控制與傳統保護的對比

傳統方法：惡意軟體黑名單

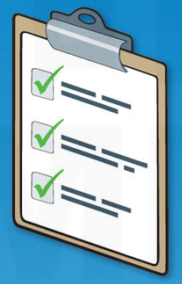
惡意軟體定義檔
數千萬以及高速增長的數量



DLoader.AMHZW \ Exploit_Gen.HOW \ Hacktool.KDY \ INF/AutoRun.HK \ JS/BomOrkut.A \ JS/Exploit.GX \ JS/FakeCodec.B \ JS/Iframe.BZ \ JS/Redirector.AH \ KillAV.MPK \ LNK/CplLnk.K ... ...

行為控制：沙箱/白名單

透過應用程式和作業系統
來定義政策進行行為控制



基於簽名的技術 只能阻止已知威脅	基於政策的技術 能夠阻止未知威脅
被動防護 無法阻止零時差攻擊	主動防護 能夠有效抵禦零時差攻擊
要求更多層面的安全防護措施配合	保護應用程式免受其它攻擊

一般伺服器主要的威脅來自於

外部威脅

- 未修正的系統
  - 作業系統
  - 應用程式
- 零時差漏洞
- 未受信任的應用程式
- 有針對性的惡意軟體

內部威脅

- 系統設定
- 惡意員工
- 粗心錯誤

保安資訊
SAVETIME
INFORMATION SECURITY

黑客針對什麼系統內容為目標?

- 機碼
- 設定檔
- 可攜式儲存裝置
- 應用程式
- 記憶體
- 作業系統

SDCS: Server Advanced

- 強制機碼完整性
- 強制檔案完整性
- 強制記憶體完整性
- 強制網路控制
- 強制網路控制
- 強制應用程式活動

保安資訊 SAVETIME INFORMATION SECURITY

主機防護四大構面

進階防護

- ✓ 應用程式白名單
- ✓ 防止零時差攻擊
- ✓ 限制作業系統行為
- ✓ 緩衝區溢位及 DLL Inject防護
- ✓ 漏洞攻擊預防

系統管控

- ✓ 鎖住組態設定值
- ✓ 防止提高系統管理員權限
- ✓ 限制裝置存取
- ✓ 防止未授權安裝
- ✓ 勒索軟體防護

網路防護

- ✓ 依應用程式限制連線能力
- ✓ 關閉後門程式
- ✓ 詳細紀錄存取資訊

稽核與告警

- ✓ 監控檔案與目錄權限變更
- ✓ 監控使用者與群組新增/修改
- ✓ 提出警示/通知，以便早期應變

Intrusion Prevention (IPS)

可以透過 Least Privilege Application Control (Sandboxing) 達到系統安全鎖定 (lockdown)

主機程式

核心系統服務

crond
RPC
LPD Printer

應用程式

Mail
Web

互動程式

RSH Shell
Browser

大部分應用程式只需要部分的系統資源及存取權限來維持其正常運作

但大部分應用系統都取得大於其原本所需之資源及權限

而攻擊隨時虎視眈眈地在尋找及利用這樣的 gap

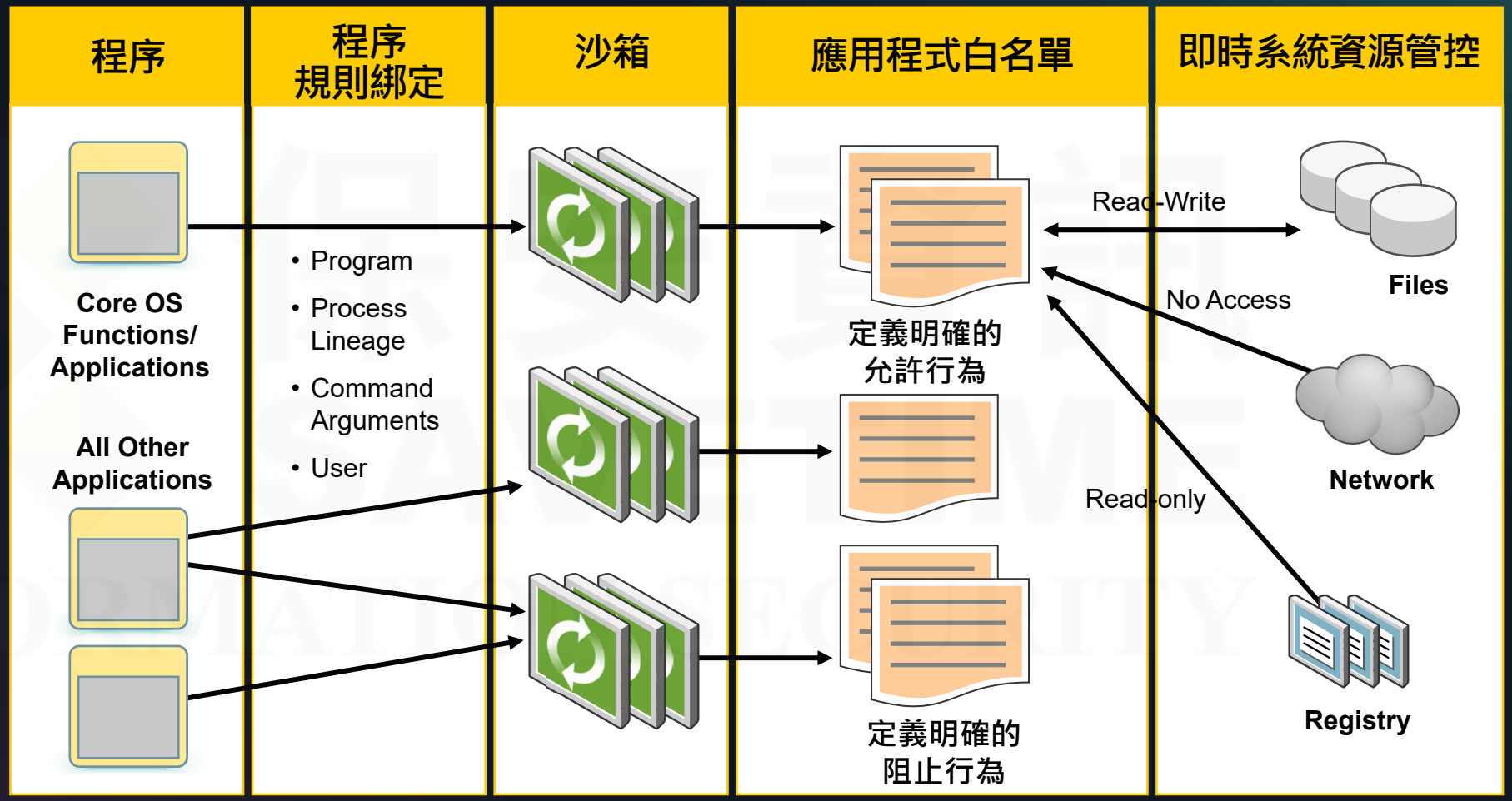
透過定義最小權限控管或被允許的資源存取政策，針對一個或多個應用程式 (processes) 建造一個 "sandbox"

精細的資源限制

檔案	讀寫資料檔案
機碼	設定資訊唯讀
網路	使用的通訊埠與裝置
設備	

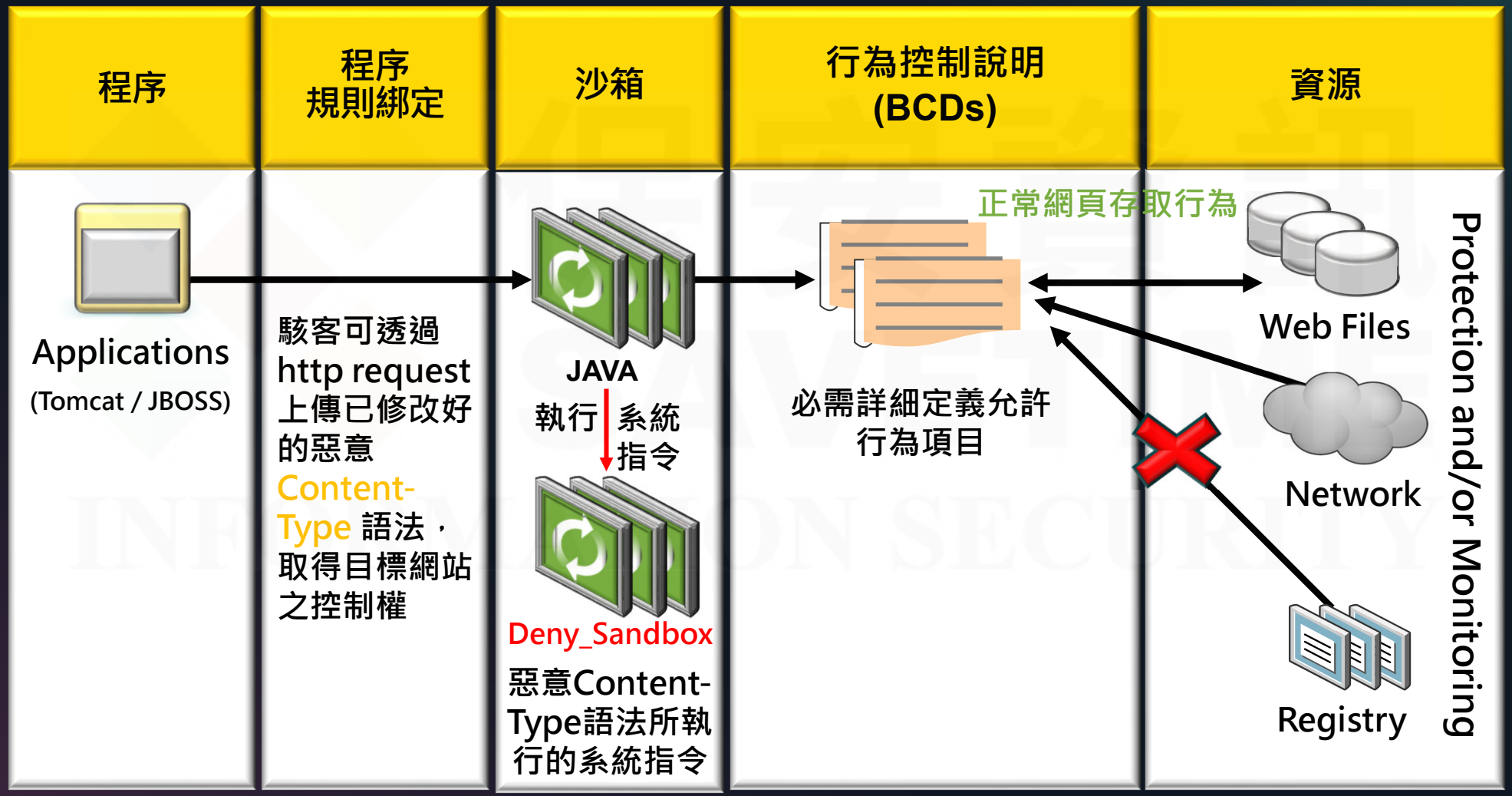
保安資訊 SAVETIME INFORMATION SECURITY

內建防護政策範本



Struts2 攻擊防護

Least Privileges Access Control (LPAC)



案例 – – Apache Struts2 攻擊手法

Struts2 攻擊語法：

allows a remote attacker to inject operating system commands into a web application through the “Content-Type” header

```
GET /struts2-blank/example/HelloWorld.action HTTP/1.1
Host: 192.168.1.11:8080
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-TW,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: haha~multipart/form-data
%{#_memberAccess=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS,@java.lang.Runtime@
getRuntime().exec("query user")};
Content-Length: 0
```

惡意指令

Source

Agent Name	2008R2_IIS7	Agent Version	6.5.0.498
Host Name	WIN-E9J1PQUE64P	OS Type	Windows
Host IP Address	192.168.1.11	OS Version	Server 2008 R2 Service Pack 1
User Name	WIN-E9J1PQUE64P\Administrator	Agent Type	CSP Native Agent

Event

Event Type	Process Assignment	Event Date	19-四月-2017 16:55:42 TST
Event Category	Real Time - Prevention	Post Date	19-四月-2017 16:56:03 TST
Operation	create	Post Delay	00:00:21
Event Severity	Warning	Event Count	1
Event Priority	45	Event ID	1144147
Acknowledgement Status	Not-Acknowledged		

Details

Description	Process Assignment for QUERY.EXE to deny_ps
Policy Name	Citrix_ESB_sym_win_whitelisting_sbp
Process	C:\WINDOWS\SYSTEM32\QUERY.EXE
Parent Process	C:\PROGRAM FILES\JAVA\JDK1.7.0_25\BIN\JAVA.EXE
Agent State	Prevention Globally Disabled, Default Policy Rule Processed
Sandbox	deny_ps
Operation	create
Process ID	2368
Thread ID	2332
Parent PID	2556
Arguments	"query" user
Process Signature	Microsoft OS Component (00039437)
Module Signature	Unsigned (00000000)
Parent Process Signature	Signed and Trusted (000384
Parent Process Publisher	Oracle America, Inc.

原始執行應用程式JAVA

惡意指令詳細參數

保安資訊 SAVETIME INFORMATION SECURITY

網路層之存取控制

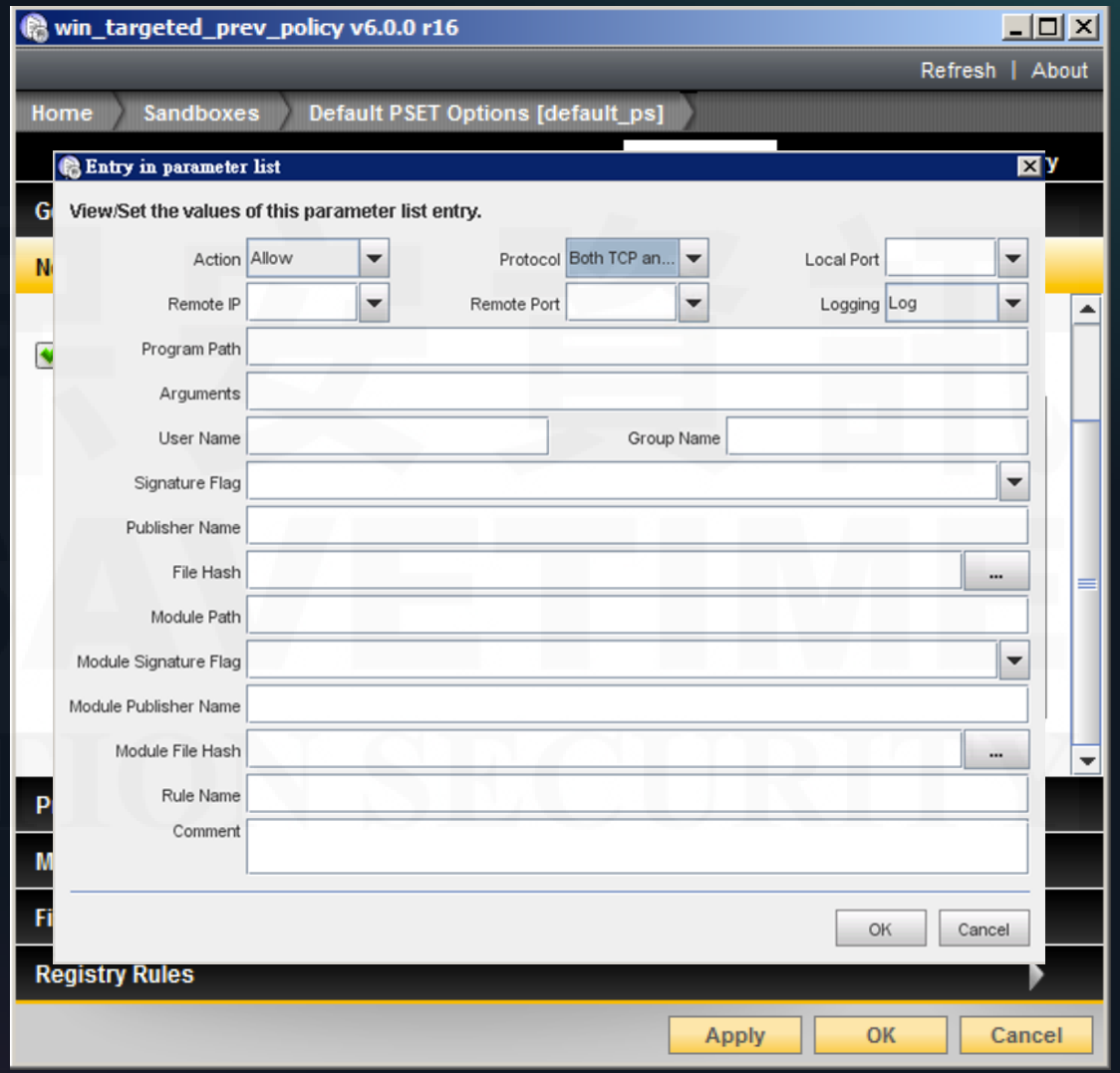
可以有效控制端點電腦上惡意程式之感染及傳播

鎖定端點電腦應用程序與特定之伺服器 IP 及 Port 進行連線，確保網路層安全

- IP 存取控制
- TCP/UDP Port 之存取控制
- 進出流量之存取控制
- 程序及參數之存取控制
- 使用者及群組之存取控制

連外網路
存取權限管控

- 受惡意軟體感染的系統洩露機密資料
- 以控制網路存取作為目標式的預防政策
- 系統與網路的連線限制



保安資訊 SAVETIME INFORMATION SECURITY

應用層之存取控制

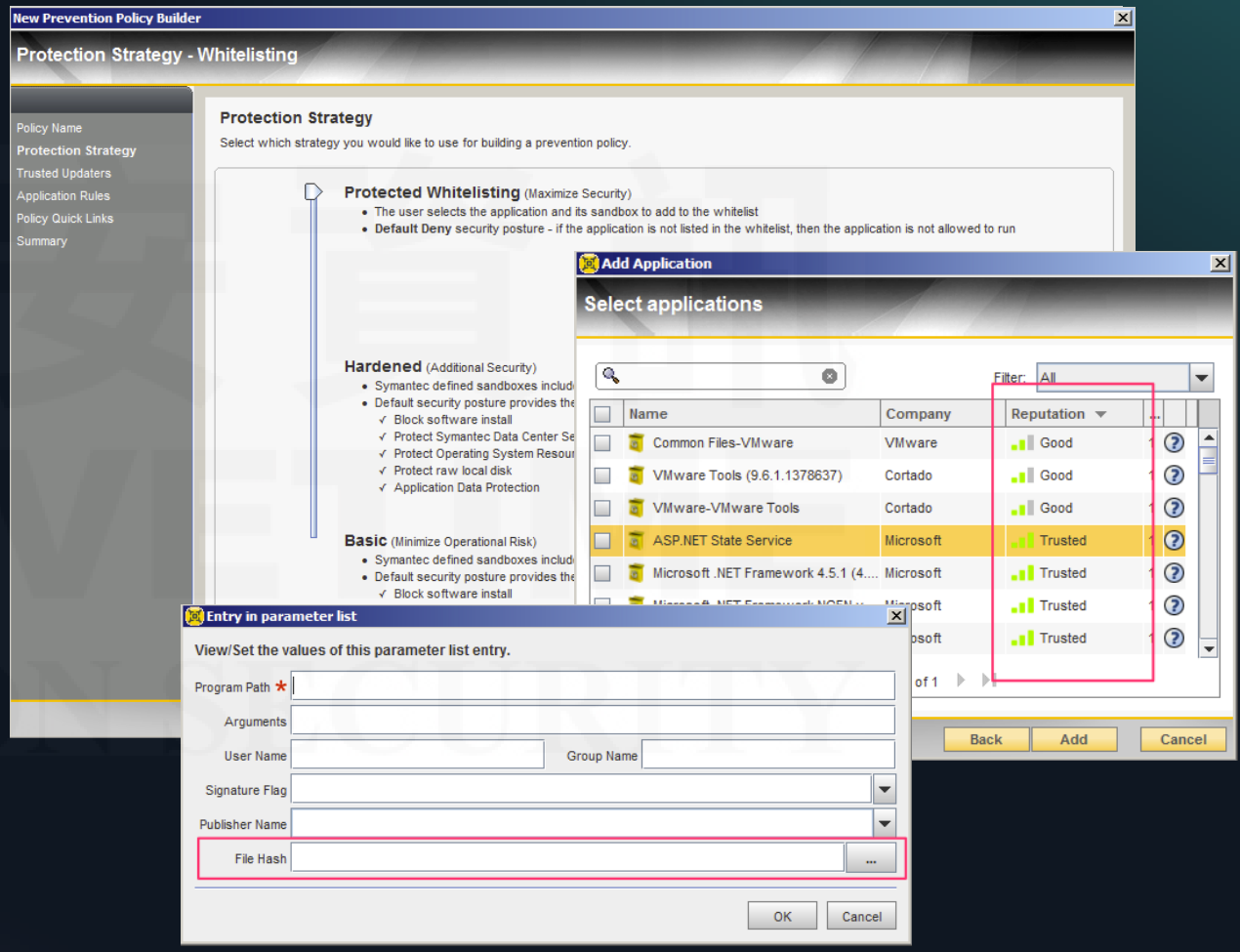
可以有效控制端點電腦之惡意程式及非法程序之執行和活動

鎖定端點電腦所需要執行之特定應用程式，自動識別系統程序與資源調用之關係，阻止可信任範圍之外的其他應用程序進行，確保應用層安全

應用程式白名單	Thread 繼承關係智能識別和控制	資源調用關係智能識別和控制	根據程序 “Sandbox” 和最小授權的行為控制

透過白名單鎖定應用程式

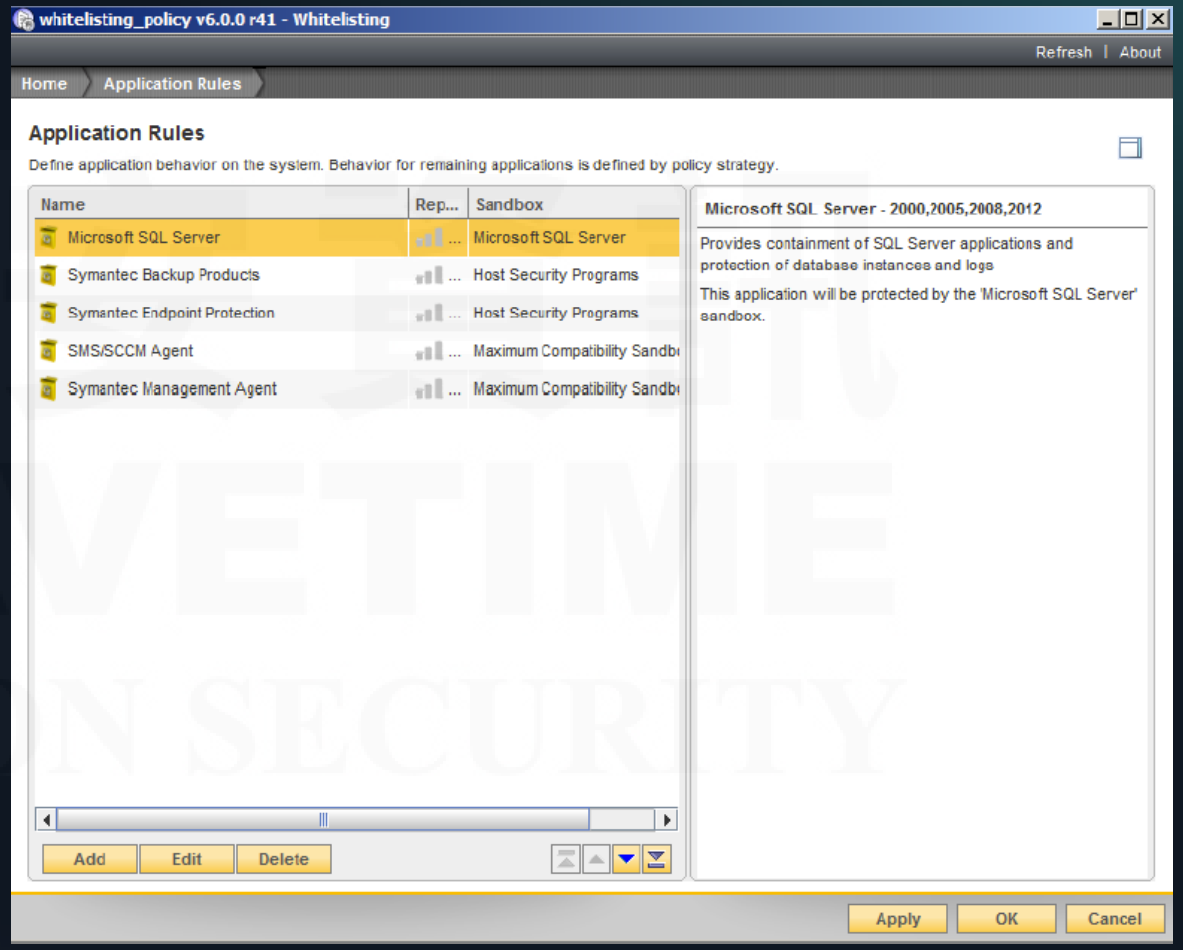
- 直觀的預防政策精靈，可減少政策建立過程中的時間和複雜性
- 政策建立期間的應用程式探索
- 賽門鐵克 **Insight** 應用程式信譽
- 使用檔案雜湊值的精細應用程式控制規則
- 使用數位簽章和受信任根憑證的常規應用程式規則



保安資訊 SAVETIME INFORMATION SECURITY

範例：資料庫鎖定

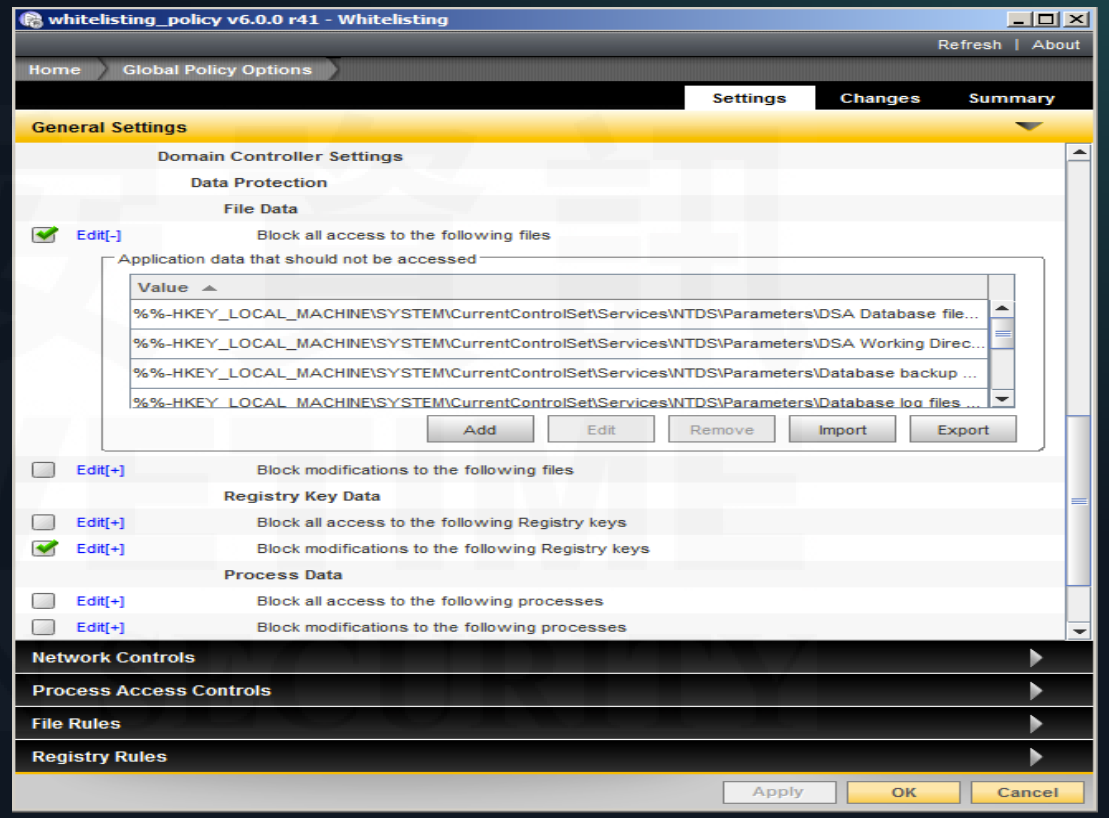
- 伺服器應該有固定的應用程序
- 只有特定的應用程式准許在 MS SQL Server 執行
- 任何互動式的使用將被拒絕
  - 網頁瀏覽器應該被阻擋
  - RDP應該被阻擋
- 只有已知的 App/Service可以更新作業系統



保安資訊 SAVETIME INFORMATION SECURITY

範例：網域控制器的鎖定

- 網域控制器一直是被攻擊目標
  - 資料庫檔案竊取 - 讓攻擊者存取到使用帳號
    - 限制存取資料庫檔案 (ntds.dit, edb.log, and temp.edb) & registry keys
- 限制透過網路存取網域控制器
  - 防止對系統的 FTP 進行存取



*SDCS:SA provides AD Server protection w/ out-of-box Policy

保安資訊 SAVETIME INFORMATION SECURITY

系統層之存取控制

可以有效保護端點電腦之更新缺失，防護入侵及零時差攻擊

鎖定系統資源與設定，開啟系統入侵防護，確保系統核心執行環境安全

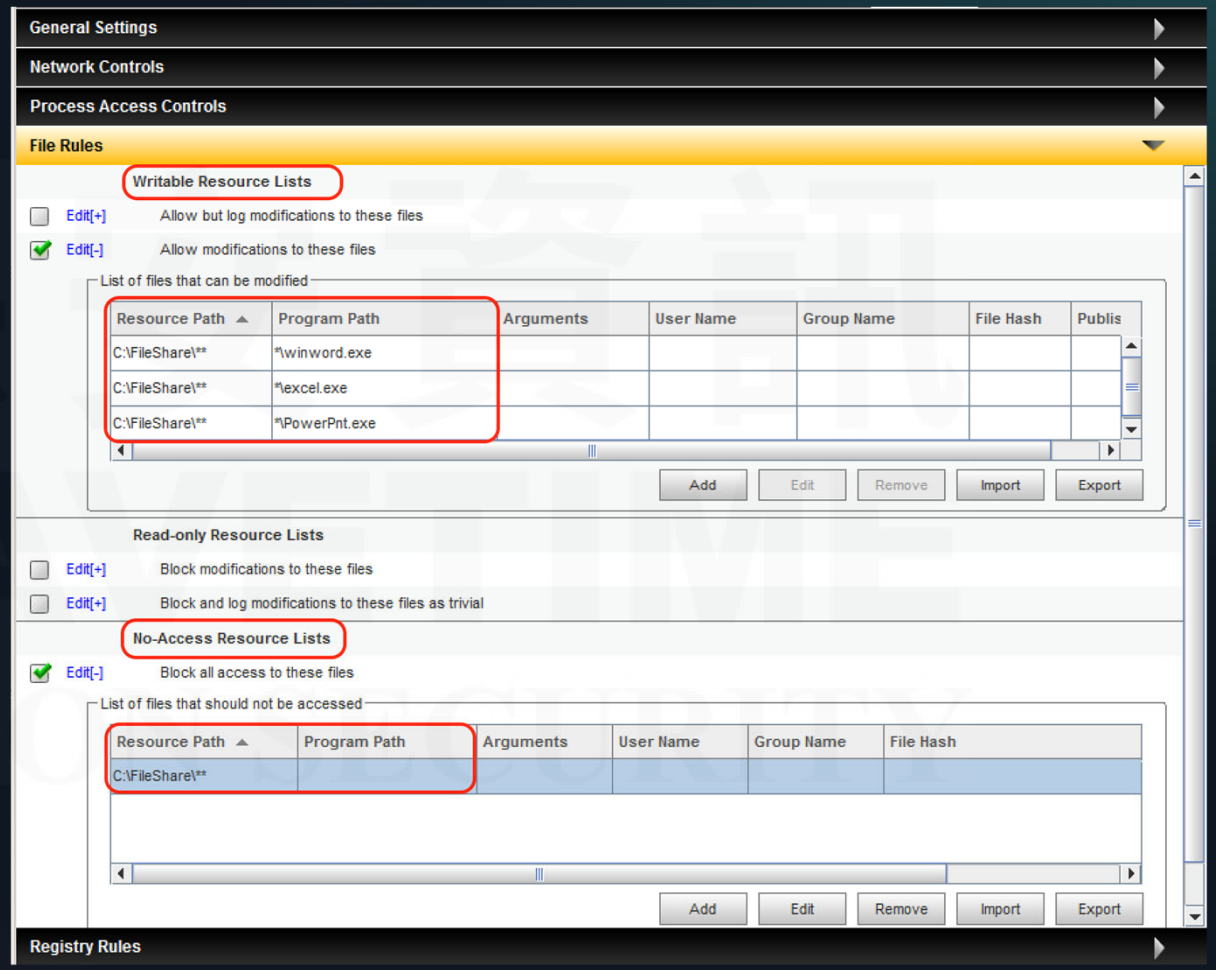
保護 Thread Injection 攻擊

保護 Buffer Overflow 攻擊

系統資源與設定之鎖定

範例：管控存取權限

- Administrator 和 root 擁用整個系統的權限
- 透過鎖定使用者 / 群組存取特定資源以降低Administrator權限
  - 使用者 / 群組只可以透過特定的程序讀取 / 寫入資源
- 對於違反鎖定資源仍受到保護

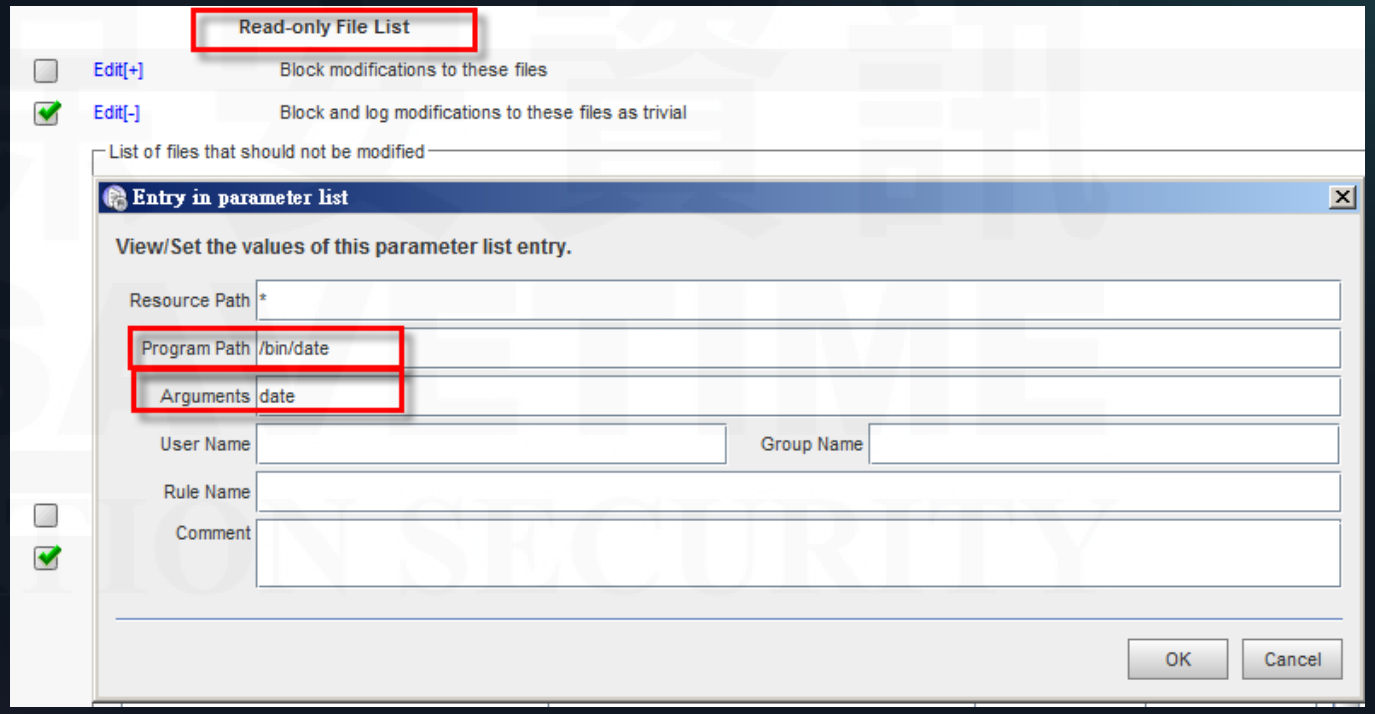


保安資訊 SAVETIME INFORMATION SECURITY

範例：系統指令參數控管

控制系統命令

- **目的**：准許使用者查詢系統時間，但不准許使用者帶時間參數，來更改系統時間
- **狀況**：使用者執行 date 可以；但不准使用者改時間 date –d 20171231



SDCS : SA Detection 稽核與告警項目

- 監控檔案與機碼變更
- 監控系統成功/失敗登入與登出紀錄
- 監控使用者與群組帳號變更
- 監控目錄與檔案權限變更
- 監控目錄權限分享變更
- 監控惡意程式/間諜程式
- 監控 USB 裝置啟動
- 網站內容監控
- AD 目錄伺服器異動監控
- Sudo 與 root 命令監控
- 賽門鐵克安全防護軟體啟動監控
- 監控 ESXi 主機設定檔與 VMX 檔案

Source

Agent Name	WINSERV-08-ENT	Agent Version	6.0.0.325
Host Name	WINSERV-08-ENT	OS Type	Windows
Host IP Address	127.0.0.1	OS Version	Server 2008 R2 Service Pack 1
User Name	WINSERV-08-ENT\Administrator	Agent Type	CSP Native Agent

Event

Event Type	File Watch	Event Date	05-Feb-2014 13:51:37 EST
Event Category	Real Time - Detection	Post Date	05-Feb-2014 13:51:38 EST
Operation	Modified	Post Delay	00:00:01
Event Severity	Warning	Event Count	1
Event Priority	59	Event ID	674
Acknowledgement Status	Not-Acknowledged		

Details

Description	Watched File Modified (c:\program files (x86)\credit card reader\data\credit_card_numbers.txt)
Policy Name	win_baseline_detection
Rule Name	Baseline_FileWatch_Sys_Other_Files_NT_Only
Operation	Modified
File Name	c:\program files (x86)\credit card reader\data\credit_card_numbers.txt
Old Size	261
New Size	293
Old Modification Date	2014-02-04 15:16:40
New Modification Date	2014-02-05 13:51:37
File Difference	SHA-256 checksum changed. Old Hash: c7c74dfaca07791b7b1416177098231f65396f152163caf66996991c671e04db New Hash: 7cdcf23a26fe3cdb2db00b4c927dae2c2f3ec41a5e187d50468474aaed5cbc4e 8a8,1 > 666666666 hacker 555-5555-5555
Session ID	1
Process Path	C:\Windows\System32\notepad.exe
Process ID	2100

保安資訊 SAVETIME INFORMATION SECURITY

安全政策 統一管理

可以滿足各種平台端點電腦 跨系統的集中安全管理需求

支援跨平台系統 安全集中管理

支援多種系統 低資源

- Winxp Embeded、Winxp、Winows7/8/10、Linux
- CPU 1%
- RAM 20M
- 檔案 100M

安全保護政策 統一管理

- 不同系統，統一設定與派送

系統安全集中監控與稽核

- 集中收集所有端點電腦之安全日誌
- 稽核報表、分析和告警

保安資訊
SAVETIME
INFORMATION SECURITY

白名單政策制訂

保安資訊 SAVETIME INFORMATION SECURITY

DCSSA佈署階段

安全狀態

階段 I

IDS 和網路控制

- 啟用開箱即用的輕量級 IDS 政策
- 啟用網路控制以隔離電腦

階段 II

針對性預防

- 為特定的伺服器服務 (Web 伺服器、網域控制器) 啟用目標式 IPS
- 獲得有針對性的 IPS，沒有誤報的風險

階段 III

學習模式(僅日誌)

- 在學習模式下啟用開箱即用的完整伺服器保護(僅限日誌)
- 允許查看完整的伺服器威脅形勢，確定特定伺服器工作負載所需的特定服務

階段 IV

全面的系統保護

- 為完整IPS防護啟用開箱即用的完整伺服器保護政策
- 根據以前的僅日誌資料與特定的伺服器服務自定義政策
- 部署更多實例驅動監控，以滿足風險/合規性/審查要求

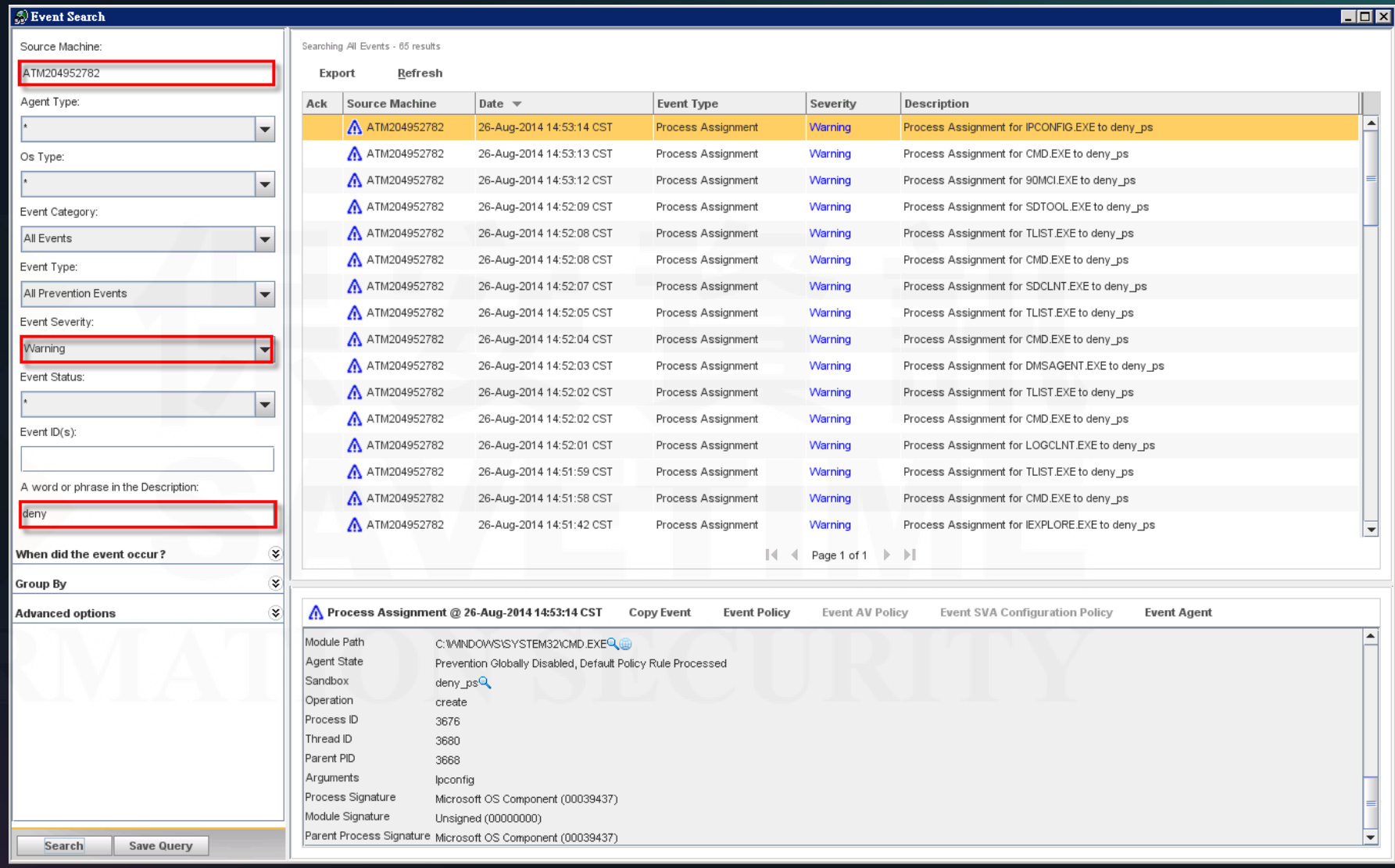
時間

Real-time Visibility and Maximum Control to Increase your Security Posture

保安資訊 SAVETIME INFORMATION SECURITY

可以透過事件檢視平台

顯示違規檔案與違反政策



保安資訊 SAVETIME INFORMATION SECURITY

透過學習模式產生白名單

Source Machine	Date	Event Type	Severity	Description
ATM204952782	26-Aug-2014 14:53:14 CST	Process Assignment	Warning	Process Assignment for IPCONFIG.EXE to deny_ps
ATM204952782	26-Aug-2014 14:53:13 CST	Process Assignment	Warning	Process Assignment for CMD.EXE to deny_ps
ATM204952782	26-Aug-2014 14:53:12 CST	Process Assignment	Warning	Process Assignment for 90MCI.EXE to deny_ps
ATM204952782	26-Aug-2014 14:52:09 CST	Process Assignment	Warning	Process Assignment for SDTOOL.EXE to deny_ps
ATM204952782	26-Aug-2014 14:52:08 CST	Process Assignment	Warning	Process Assignment for TLIST.EXE to deny_ps
ATM204952782	26-Aug-2014 14:52:08 CST	Process Assignment	Warning	Process Assignment for CMD.EXE to deny_ps
ATM204952782	26-Aug-2014 14:52:07 CST	Process Assignment	Warning	Process Assignment for SDCLNT.EXE to deny_ps
ATM204952782	26-Aug-2014 14:52:05 CST	Process Assignment	Warning	Process Assignment for TLIST.EXE to deny_ps
ATM204952782	26-Aug-2014 14:52:04 CST	Process Assignment	Warning	Process Assignment for CMD.EXE to deny_ps
ATM204952782	26-Aug-2014 14:52:03 CST	Process Assignment	Warning	Process Assignment for DMSAGENT.EXE to deny_ps
ATM204952782	26-Aug-2014 14:52:02 CST	Process Assignment	Warning	Process Assignment for TLIST.EXE to deny_ps
ATM204952782	26-Aug-2014 14:52:02 CST	Process Assignment	Warning	Process Assignment for CMD.EXE to deny_ps
ATM204952782	26-Aug-2014 14:52:01 CST	Process Assignment	Warning	Process Assignment for LOGCLNT.EXE to deny_ps
ATM204952782	26-Aug-2014 14:51:59 CST	Process Assignment	Warning	Process Assignment for TLIST.EXE to deny_ps
ATM204952782	26-Aug-2014 14:51:58 CST	Process Assignment	Warning	Process Assignment for CMD.EXE to deny_ps
ATM204952782	26-Aug-2014 14:51:42 CST	Process Assignment	Warning	Process Assignment for IEXPLORE.EXE to deny_ps

Event Wizard...
Not Acknowledge

Multi Event wizard

Event Grouping

Group the selected events by: Process Type

Group Name	Event Count
PROCEXP.EXE - Windows, version 6.x	1
VMACTHLP.EXE - Windows, version 6.x	9
UPHCLEAN.EXE - Windows, version 6.x	9
VMWARESERVICE.EXE - Windows, version 6.x	9
WINVNC.EXE - Windows, version 6.x	11
VMWARETRAY.EXE - Windows, version 6.x	5
VMWAREUSER.EXE - Windows, version 6.x	5
WINZIP32.EXE - Windows, version 6.x	1
SISIPSTRAY.EXE - Windows, version 6.x	5
SISEVENTVIEWER.EXE - Windows, version 6.x	2
SNAGIT725.EXE - Windows, version 6.x	9
WRAR393.EXE - Windows, version 6.x	1
FILEZILLA_SERVER-0_9_43.EXE - Windows, version 6.x	5
UEDIT32.EXE - Windows, version 6.x	1

Back Next Cancel

透過 Import CheckSum 產生白名單

1 Checksum C:\123.txt C:\

2

HashValues_1409071710559.csv - 記事本

檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

```
MD5,SHA256 7312c4b314b8aed61a8b92367cf008e1, b3b121ccac92a71152d3aa6a783927d4, eb39a24cd08bc818edad1f59867e5646,
87f88b9c8882e84344729ddbea731bd8, feed731d80e4cccc5be0a5308552d178, 9c17dcd6ddfeb1a012544faf4f2789f6,
ba073edde13179da2deff264c2a272ab, 2110ce8cb4c6937200a973ad0b70f33d, dd2eb5e64619613c4c108cfb192f4950,
a02ee61542caae25f8a44c9428d30247, afa10db13b9a0537297aeef2cd66352f, 841736fab112ac493646e4399e684d38,
0c8f794b0c057eb421569a4e5b8e98c5, 942cae96436ffea01bfb098ca08f2ee8, 6462203a329e317bb12fb222eec1a107,
```

3

File Hash Editor

Specify File Hash Values

MD5	SHA256
7312c4b314b8aed61a8b92367cf008e1	
b3b121ccac92a71152d3aa6a783927d4	
eb39a24cd08bc818edad1f59867e5646	
87f88b9c8882e84344729ddbea731bd8	
feed731d80e4cccc5be0a5308552d178	
9c17dcd6ddfeb1a012544faf4f2789f6	
ba073edde13179da2deff264c2a272ab	
2110ce8cb4c6937200a973ad0b70f33d	
dd2eb5e64619613c4c108cfb192f4950	
a02ee61542caae25f8a44c9428d30247	

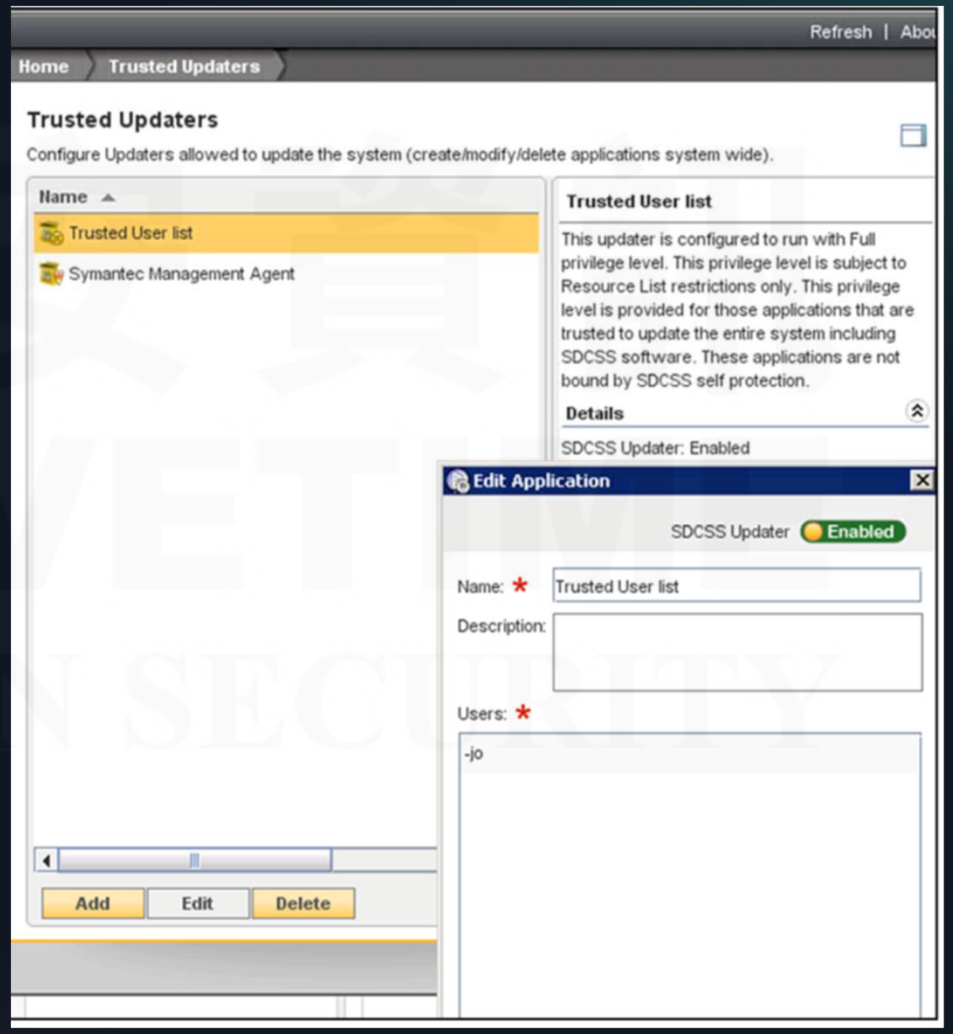
Add Delete Import Export

OK Cancel

Trusted Update -- 信任下載更新

Trusted Update

- 是否准許系統更新
- 只有更新程式可以執行
- Trusted Updater 可以被准許執行：新增、修改、刪除等動作



保安資訊
SAVETIME
INFORMATION SECURITY

常見防護情境
(Use Case)

保安資訊 SAVETIME INFORMATION SECURITY

SDCS 到底可以幫助客戶解決什麼問題呢?

可能的問題	解決方式	價　值
APT 攻擊	• 發現違反相關的資安控管 • 發現可疑管理者或入侵者之行為	• 保護系統不受 APT 攻擊
EOL 軟體保護	• 系統鎖定。控管存取系統資訊限制。 • 停止不必要服務連線	• 縱使沒有漏洞修正程式更新，也可以避免該風險產生
Web Server 網頁置換攻擊	• 偵測 Web Server 網頁路徑檔案之更改 • 阻擋 Web Server 網頁路徑檔案之更改	• 保護 Web Server 避免遭受網頁置換攻擊
各作業平台系統強化	• 透過重要系統檔案保護與設定檔管控。可以強化系統整體安全	• 保護重要系統 (防毒管理主機、SCCM、AD、Exchange Server、Web Server、Database Server、Application Server) 之資料檔案及設定檔避免非授權之更改

SDCS 到底可以幫助客戶解決什麼問題呢?

可能的問題	解決方式	價　值
法規遵循	• 提供標準安全政策範本 • 針對檔案、機碼、程序異動可以提供日誌與報表分析	• 透過標準政策範本符合法規要求 • PCI要求
VMs 及 Hypervisor 之安全	• 監控 Hypervisor 設定檔之更改以及防護鎖定 VM guests 系統	• 根據 VMWare 建議之強化手冊原則，加強 VMWare Hypervisor 及雲端之安全 • 集中控管虛擬及實體環境之安全
事件根因調查	• 保護重要系統稽核紀錄，並即時收集至管理中心，避免資料被竄改及刪除	• 即時並集中收集資安相關事件至管理中心資料庫，於事中發現任何異常之行為時進行自動通報，並於事後協助管理者及調查人員找出資料外洩或入侵之根因

主要功能概述

- 零時差攻擊防護
- 應用程式白名單
- 帳號監控
- 分享目錄監控
- 目錄與檔案監控
- 目錄權限異動監控
- 網頁竄改防護
- 監控系統所有的執行程式
- 應用程式日誌檔的監控
- 主機機碼的監控
- 主機連線/登入失敗的監控
- 族繁不及備載.....

保安資訊
SAVETIME
INFORMATION SECURITY

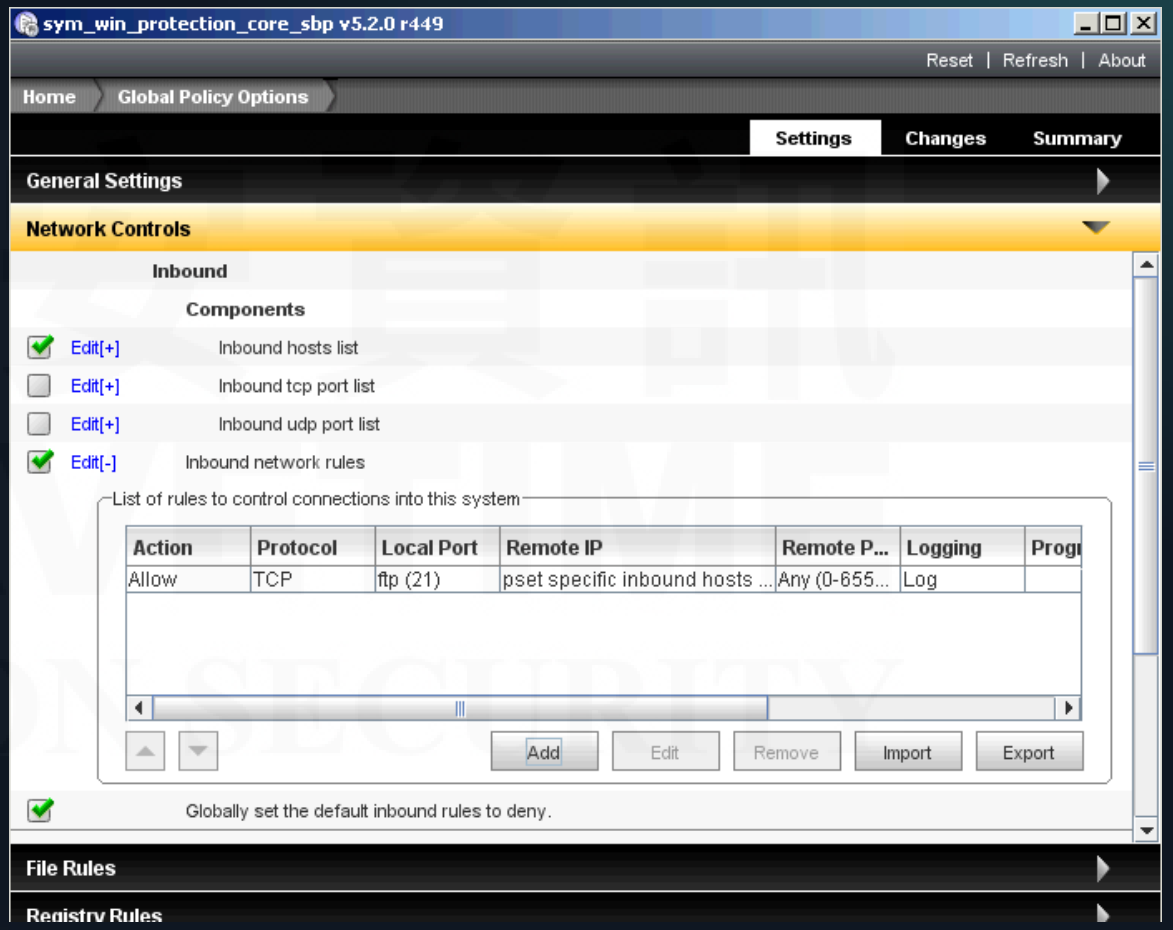
總 結

保安資訊 SAVETIME INFORMATION SECURITY

限制所有網路之進出管道

APT 很多時候會利用系統的安全設定不周全，可能只是很簡單的網路連線限制，就可以阻擋很多 APT 於 Discovery 階段所進行之行為，如果只限制授權之系統進行連線，將大幅減少系統被 Compromise 的機會

網路層防火牆通常不足夠保護於 APT 攻擊時所進行之內部系統探測及攻擊行為，Host Based 防火牆得以進階限制進出系統之 traffic

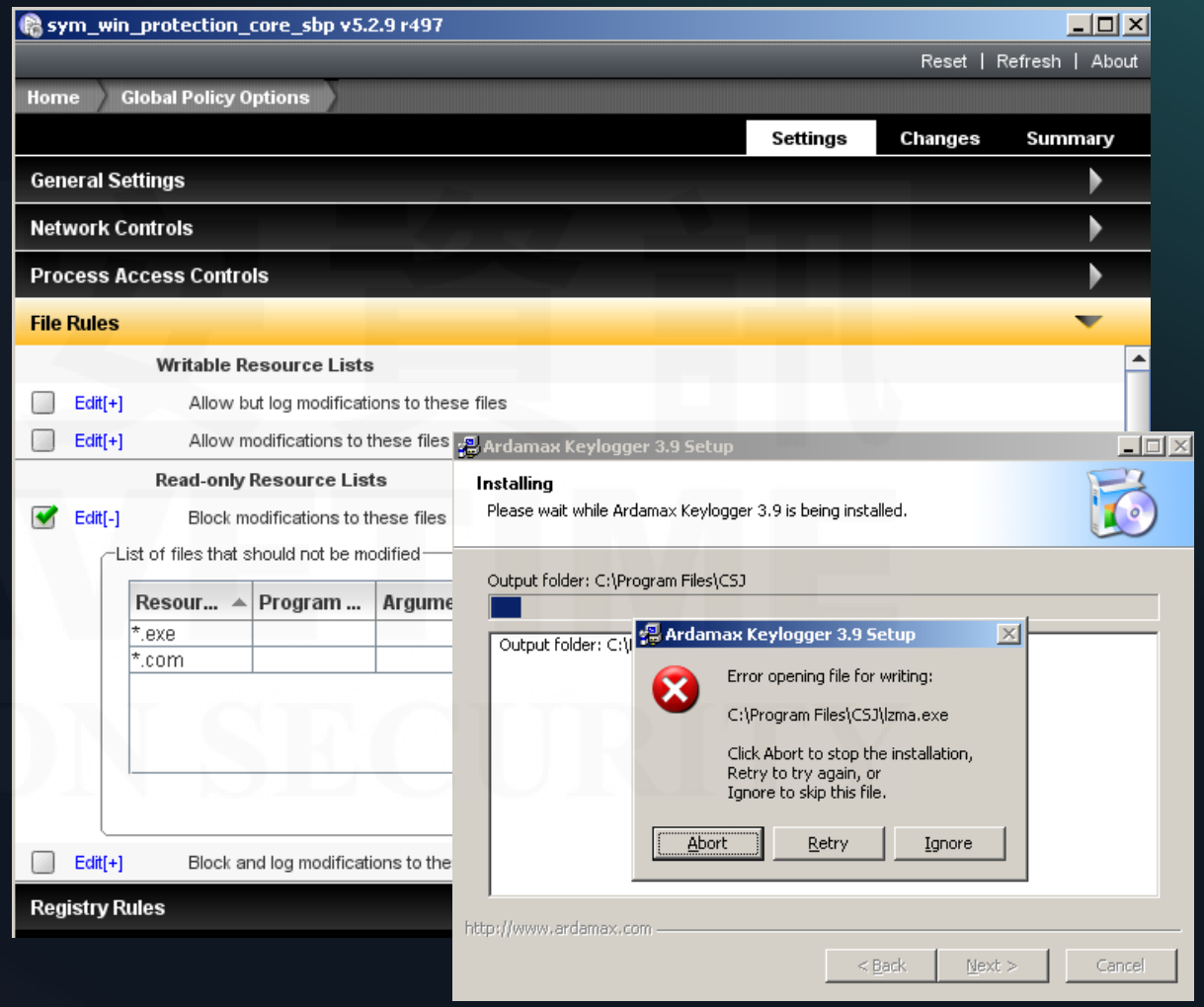


保安資訊 SAVETIME INFORMATION SECURITY

保護系統免於被非法安裝非授權之應用程式

APT 於 Discovery/Capture 階段，會安裝rootkit、keylogger、sniffer或backdoor軟體，得以在內部網路內獲取更多資訊以及拿下更多關鍵系統。

弱點被利用、連線密碼檔被取得或是密碼檔暴力破解後，通常會取得管理者權限，且也具有安裝程式或服務的權限，導致系統整個被接管

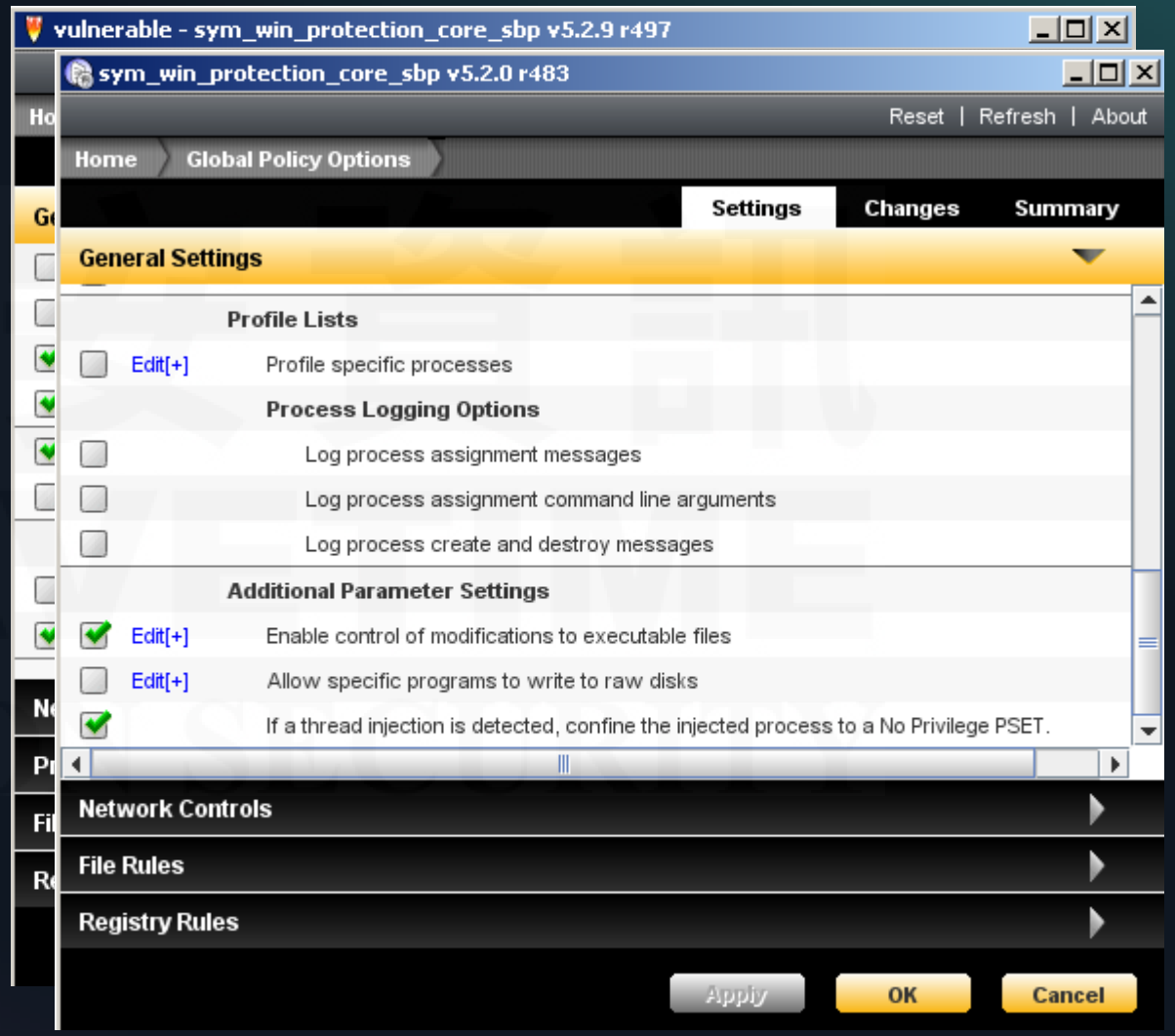


保護利用記憶體或程序之攻擊

APT 於 Capture 階段，通常會利用系統或服務之弱點，進行Buffer Overflow或 Thread Injection 攻擊。

這些攻擊可以透過合法但具有弱點之服務或程序，將另一個非法之指令注入至記憶體空間裡，以使其被執行起來。

如果特定之服務或程序，超出原本可以執行之範圍，就有可能因為弱點被利用，而安裝惡意程式或關閉其他特定程序，進而在該系統上取得更多利用及攻擊的空間。

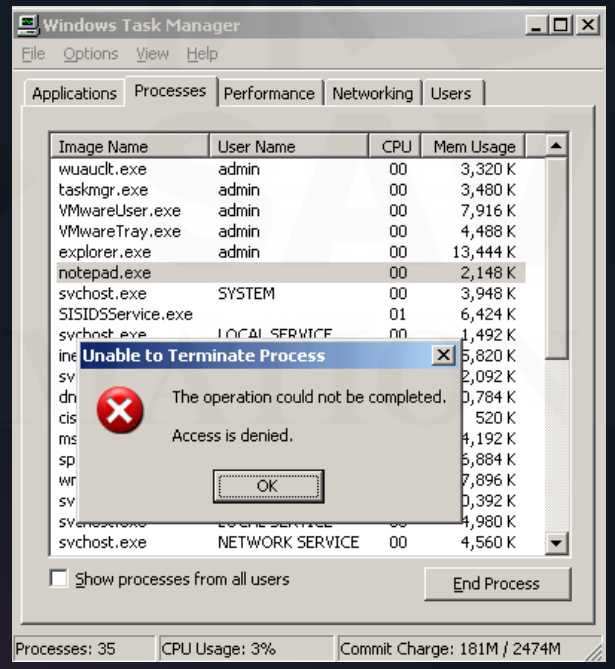


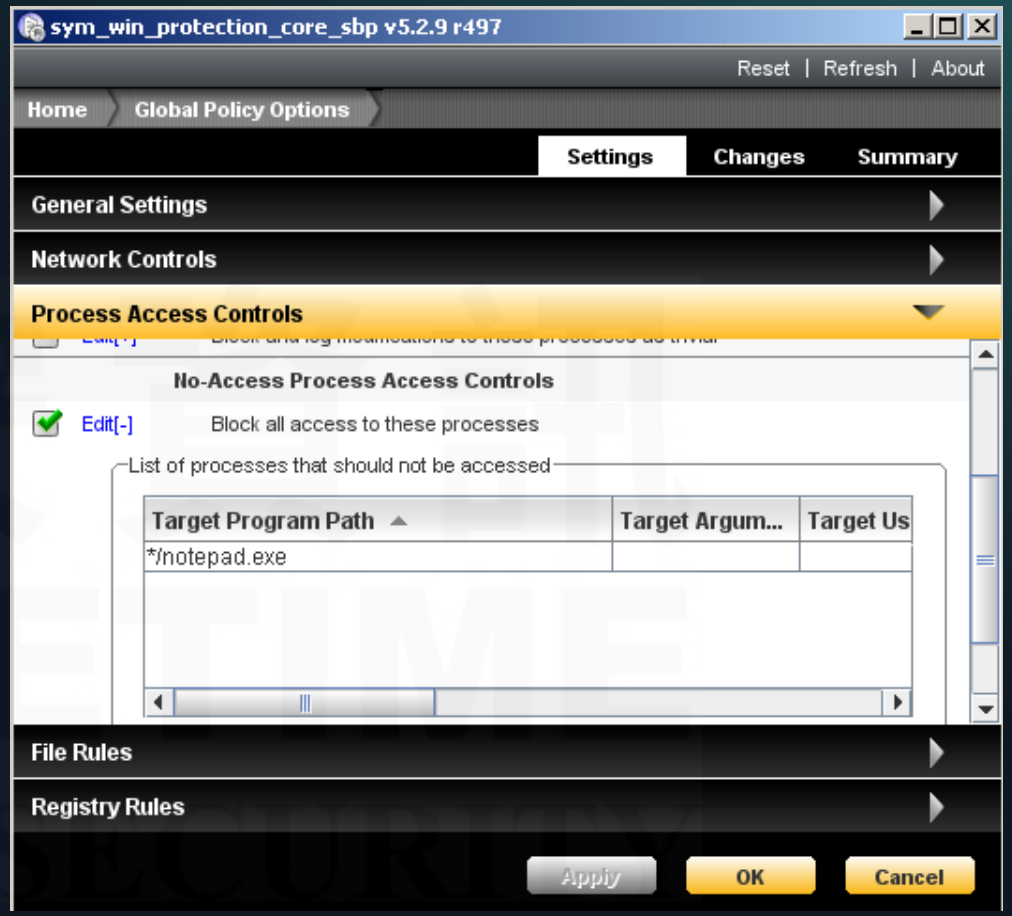
保安資訊 SAVETIME INFORMATION SECURITY

保護系統提供之服務或安全保護軟體之程序不被停用

APT，通常會透過系統弱點之利用，並於提升權限後，於 Discovery 階段，**將安全保護軟體之程序進行停用**，以利進行惡意程式之安裝，或於最後 Exfiltration 之階段，避免安全軟體偵測。

若攻擊目標為癱瘓系統，也可能於最後階段進行系統服務之停用。

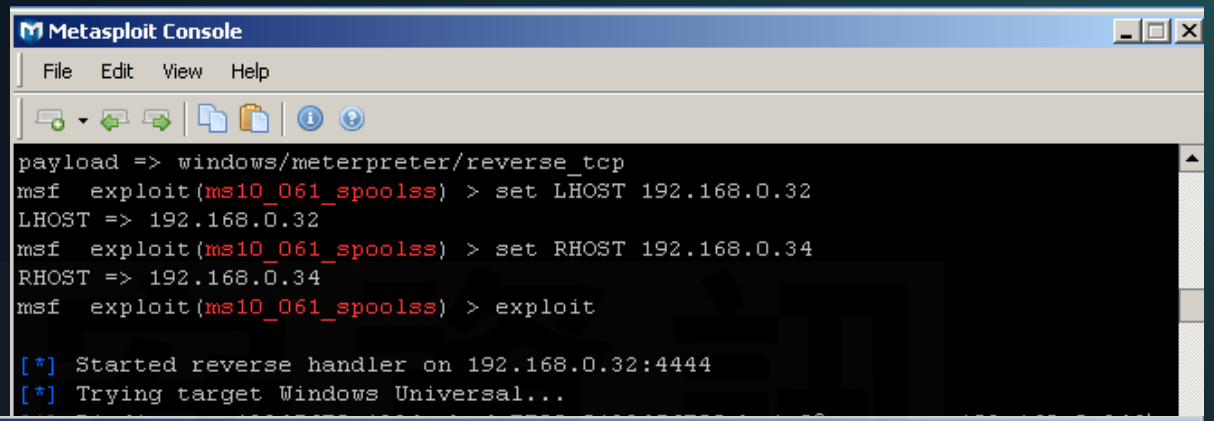


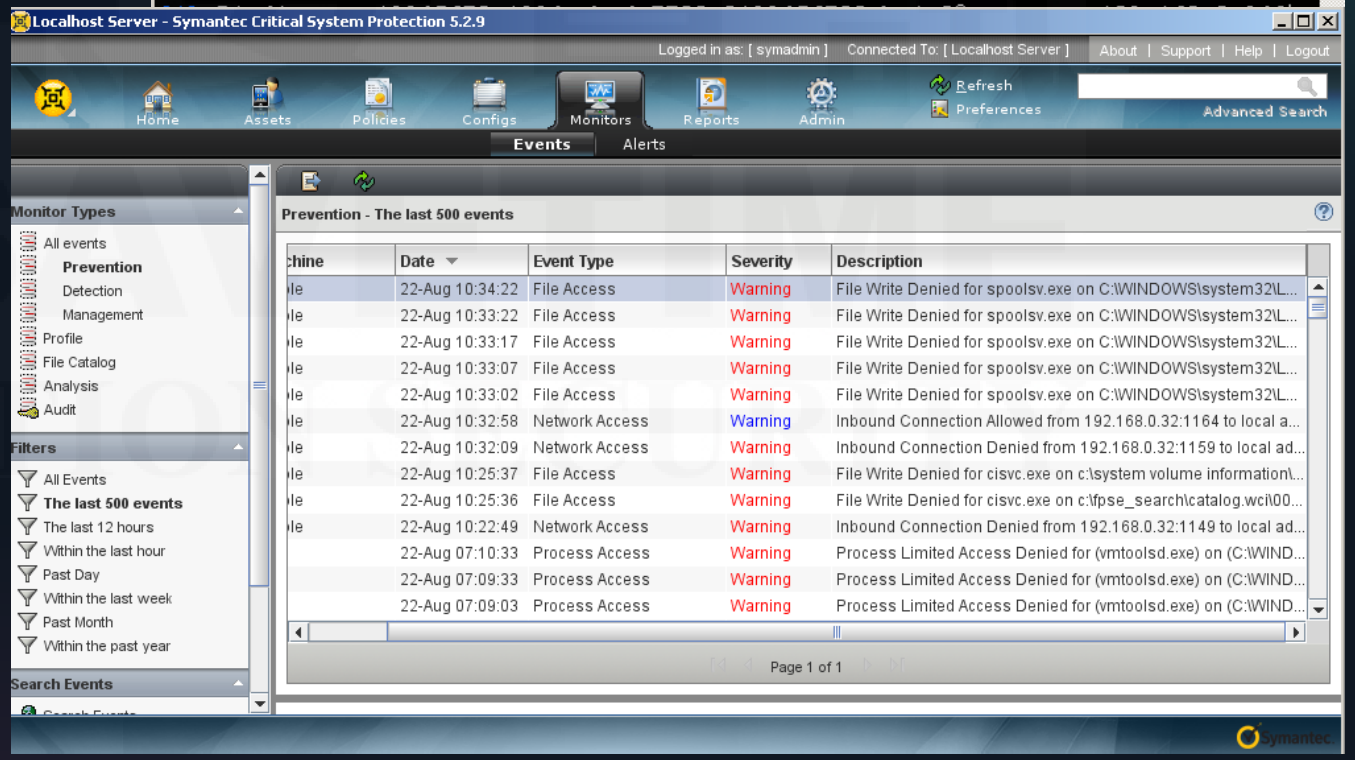


保安資訊 SAVETIME INFORMATION SECURITY

針對零時差攻擊進行保護

APT 於 Incursion/Discovery 最常出現的步驟，就是利用系統之存在之弱點，一旦服務或系統之弱點被利用，通常遠端連線或遠端指令就可以被建立或執行，接下來就會安裝其他執行檔或惡意程式至該系統，以取得下一階段之攻擊準備或直接取得系統重要資料。





保安資訊 SAVETIME INFORMATION SECURITY

黑帽大會上進行實際驗證

透過 DCS 保護具有漏洞之資料中心系統，提供 $5,000 美金獎金，驗證其無法被入侵

- **Setup** – "Mini Data Center" of Windows 2000 & 2003 servers, RHEL, CentOS, desktops (Windows XP and 7)
  - POS軟體安裝在Desktop上，連線至Server處理交易資料
  - DCS：SA 故意將防火牆全開
  - 故意不修補存在的弱點
- **Goal** – "capture the flag" (取得存取權限並取得資料) 即可贏得獎金
- **Players** – 同時超過 40 位參賽者, 其中包含美國國防部、俄國及中國的駭客
- **Attacks** – 應用很多技術，包含：
  - 暴力密碼猜測工具 (每分鐘超過 400 次的密碼猜測行為)
  - Metasploit 相關漏洞利用工具
  - 嘗試透過 Symantec online help system 停用 DCS:SA 服務
- **Results** – 驗證 DCS 能保護所有系統，$5,000 美元獎金仍未被頒發!

保安資訊 SAVETIME INFORMATION SECURITY

DCSA系統需求

Management server and UMC

硬體

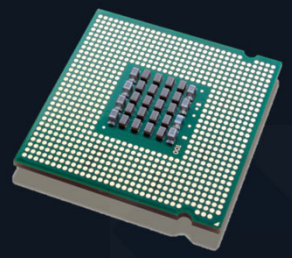
60 GB 可用空間（全平台）
8 GB RAM
4 CPUs
註：對於 SQL Server 的企業版，必須至少有 60 GB 的可用磁碟空間。這僅適用於全新安裝。其他版本的 SQL Server 至少需要 1 GB 的可用磁碟空間。但是，如果要使用 SQL Server 的企業版升級管理伺服器，則必須具有等於當前使用的磁碟空間量 + 60 GB 的可用磁碟空間。

軟體

Windows 2012 R2 以上版本
Microsoft SQL Server 2008 以上版本
.NET Framework 4.0 or 4.5.1
PowerShell 2.0

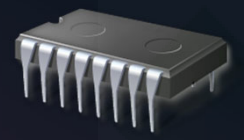
其他詳細內容請參考：
https://knowledge.broadcom.com/external/article/214933

Agent所需負擔最小

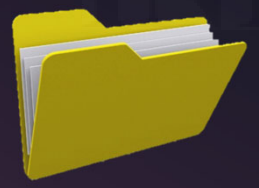


- **Typical CPU Usage**

  1-6% depending upon policies used and the amount of IO usage on the system



- **Memory**
  - Windows - typically 25-40MB
  - Unix – typically 40-80MB



- **Disk space**
  - Requires a minimum of 100MB disk space
  - Additional disk space may be used if agent log files are not purged periodically

保安資訊
SAVETIME
INFORMATION SECURITY

感謝您！

保安資訊有限公司

電話：
0800-381500
04-23815000

網站：
www.savetime.com.tw

保安資訊
SAVETIME
INFORMATION SECURITY

附錄
(內建政策)

保安資訊 SAVETIME INFORMATION SECURITY

IPS

內建政策分 Windows 及 Unix (Unix/AIX/Linux)

- **Windows**
  - null：sym_win_null_sbp 不為 Agent 提供保護、不記錄違反政策、預設，Agent註冊時自動套用；支援所有Windows作業系統。
  - OS：為Windows 作業系統和常見應用程序提供基本保護，同時為所有其他程序提供高度兼容的環境
  - Workload：說明如後
- **Unix (Unix/AIX/Linux)**
  - null：sym_unix_null_sbp 不為 Agent 提供保護、不記錄違反政策、預設，Agent 註冊時自動套用；支援所有 Solaris 和 Linux 作業系統。
  - OS：提供應用程序和核心作業系統守護程序 (daemons) 特定的行為控制描述以及特別受限的互動程序。其他的daemons和交互程序則是使用標準的權限。
  - Workload：為特定的工作負載定義一個沙箱
    Apache / PHP (sym_unix_apache_workload_sbp)
    MySQL (sym_unix_mysql_workload_sbp)

參考：DCSSA_Prevention_Policy_Reference_Guide.pdf

Windows Workload Prevention Policy

Workload 政策是以基本 [Windows] 入口點保護 (EPP) 政策和自定義預防政策做為每個工作負載的政策。以類似於 6.0 Windows Prevention Policy（使用強化策略），但不包括套用於 Internet Explorer、IIS、Exchange 等應用程序的沙箱。因此，它的意思是可作為基本政策。自定義預防政策的工作負載也就是從應用程序沙箱轉換來的。

- Windows Entry Point Protection (sym_win_entry_point_protection_sbp)
- MS Exchange (sym_win_exchange_workload_sbp)
- Internet Explorer (sym_win_iexplore_workload_sbp)
- Internet Information Services (IIS) (sym_win_iis_workload_sbp)
- MS Office (sym_win_msoffice_workload_sbp)
- MS SQL Server (sym_win_mssqlsrv_workload_sbp)
- Oracle (sym_win_oracledb_workload_sbp)
- Outlook and Outlook Exchange (sym_win_outlook_workload_sbp)

套用這些Workload政策時需要與Windows Entry Point Protection policy 一起搭配使用

參考：DCSSA_Prevention_Policy_Reference_Guide.pdf

政策的策略

policy strategies

無論選擇何種政策，6.0的政策都會自動限制已知的作業系統組件。一個預設政策中使用構建的沙箱集來限制作業系統組件並限制僅能存取那些所需的系統資源。

Basic strategy 基本策略

為作業提供保護系統和一組常見的應用程序，其他則受到限制。

預設啟用保護類別：

- 遵守全域資源列表限制
- 軟體安裝限制
- 阻止對可執行檔的修改
- 阻止修改啟動資料夾
- 阻止註冊 COM 和 ActiveX 物件

參考：DCSSA_Prevention_Policy_Reference_Guide.pdf

Hardened strategy 強化策略

政策的策略

policy strategies

除為作業系統和一組常見應用程序提供保護外。此策略將其餘應用程序（服務和交互式程序）限制在強化沙箱內。強化沙箱設置為限制程序執行，這樣就不能任意修改作業系統或其他應用程序資源。

預設啟用保護類別：

- 遵守所有其他應用程序資料限制
- 遵守全域資源列表限制
- 軟體安裝限制
- 阻止對可執行檔的修改
- 阻止修改啟動資料夾
- 阻止註冊 COM 和 ActiveX 物件
- 基本作業系統限制
- 保護自動啟動位置
- 保護作業系統資源
- 保護原始本機磁碟設備

參考：DCSSA_Prevention_Policy_Reference_Guide.pdf

Protected Application Control strategy 應用程式白名單

政策的策略

policy strategies

為作業系統提供保護，並禁止啟動應用程序，策略配置中明確列出的應用程序除外。
需自行新增應用程序及其沙箱。

為了使作業系統能正常執行，預設在 %systemroot% 目錄或子目錄之外的任何含 Microsoft 數位簽章的程序都會在 Default Windows Programs and Services 沙箱裡執行。

若要限制這些程序執行，可以執行以下任一步驟：

- 在 Default Windows Programs and Services 沙箱中編輯 Sandbox Execution 選項，並將程序新增到 Programs the Default Windows Services may not run 列表或者
- 在 Application Rules 頁面上為程序建立一個應用程序，然後選擇 Deny sandbox 選項。

參考：DCSSA_Prevention_Policy_Reference_Guide.pdf

其他更詳細的說明請參考文件
DCSSA_Prevention_Policy_Reference_Guide.pdf

以上檔案在 SDCS Related Documents 壓縮檔內