

入侵防禦系統（Intrusion Prevention Systems，IPS）發展至今大約十年的時間，其技術也從傳統黑盒子般的系統，演進至新世代智慧型入侵防禦系統。傳統入侵防禦系統為人所詬病的大量日誌、人為介入、報表無參考性等問題，都在新世代入侵防禦系統獲得解決。

## 縱深防禦：從外到內完整防護

為了改善傳統入侵防禦系統的問題，Sourcefire新世代入侵防禦系統具備網路狀態探索、自動調校規則、使用者身份識別及關連式分析報表等新功能，並且允許管理者自行撰寫入侵防禦規則，防護自行開發的應用程式，或是已經停止支援的產品。

Sourcefire入侵防禦解決方案包含Sensor（IPS）及Defense Center（管理主控台），Sensor除了部署在網路邊界，還能防護內部網段、DMZ區、資料中心…等位置，提供完整的縱深防護；一般傳統的入侵防禦系統都部署在閘道端，無法防禦內部攻擊，造成很大的資安漏洞。

以下我們簡單說明Sourcefire跨世代的防禦技術：

- 即時網路警知（RNA，Real-time Network Awareness）

RNA是透過Sourcefire獨家的被動探索技術，分析通過Sourcefire IPS的封包，以獲得最即時的内容，包含網路設備、作業系統、應用程式、行動裝置及網路流量等資訊。由於採用被動式探索技術，因此不會造成任何負擔，主機上也不會產生任何安全警示（主動探索可能會造成網路斷線，引起防火牆或防毒軟體的警示，並且有空窗期的問題）。

舉例來說，當一台新的電腦插上網路線，封包流經Sourcefire IPS後，系統就開始分析相關的内容，包含NetBIOS名稱、MAC位址、作業系統、開啟的服務、使用者及可能的弱點，也就是說，它能讓管理者隨時掌握企業網路的一舉一動。

- 自動調校（Auto-Tuning）規則

一般而言，為了效能與防護效率的考量，入侵防禦系統並不會開啟全部的防護規則，而且要隨著特徵資料庫的更新，定期調校規則，這也是入侵防護系統耗費最多人力之處。

而透過上述RNA的資訊，Sourcefire就能夠知道網路上有哪些裝置，並依此來制定防護規則。Sourcefire可以採全自動方式，自動套用要啟用的規則，或是透過「半自動」的方式，由管理者過濾要啟用哪些規則，彈性調整設定以符合環境需要。

- 即時使用者警知（RUA，Real-time User Awareness）

人是電腦犯罪事件的肇事者/受害者，當發生資安事件時，要找的不是電腦或IP，而是使用者，特別是在DHCP或多人共用電腦的環境，需要花費許多功夫才能找出當時的使用者。Sourcefire支援AD、LDAP、IMAP及Oracle…等使用者資訊，方便管理者在事件日誌中，即時查看使用者的資訊。

| 主要特性          | 傳統IPS | 新世代IPS |
|---------------|-------|--------|
| 主動IPS及被動IDS模式 | ✓     | ✓      |
| 基本偵測政策        | ✓     | ✓      |
| 報告、警報及主控台     | ✓     | ✓      |
| 客制化規則         |       | ✓      |
| 以弱點為基礎的防護     |       | ✓      |
| 自動化的影響評估      |       | ✓      |
| 自動調校          |       | ✓      |
| 應用程式政策管理      |       | ✓      |
| 網路行為分析        |       | ✓      |
| 使用者政策管理       |       | ✓      |
| 虛擬IPS及管理主控台   |       | ✓      |



Sourcefire新世代入侵防禦系統，除了管理主控台及IPS之外，還包含四種感知技術，並支援虛擬化及SSL檢查，達到最高等級的安全防護。

### • 整合Snort防護規則

很多企業擁有自行開發的系統，或是已經停止支援的作業系統、應用程式，而成為資安防護的孤兒，因為入侵防禦系統廠商不會為了這些系統而去開發攻擊特徵。Sourcefire 採用 Snort 防護引擎，可自行撰寫防護規則，也可以直接匯入網路上發布的規則，更是業界唯一能夠完整匯入Snort規則的入侵防禦系統。

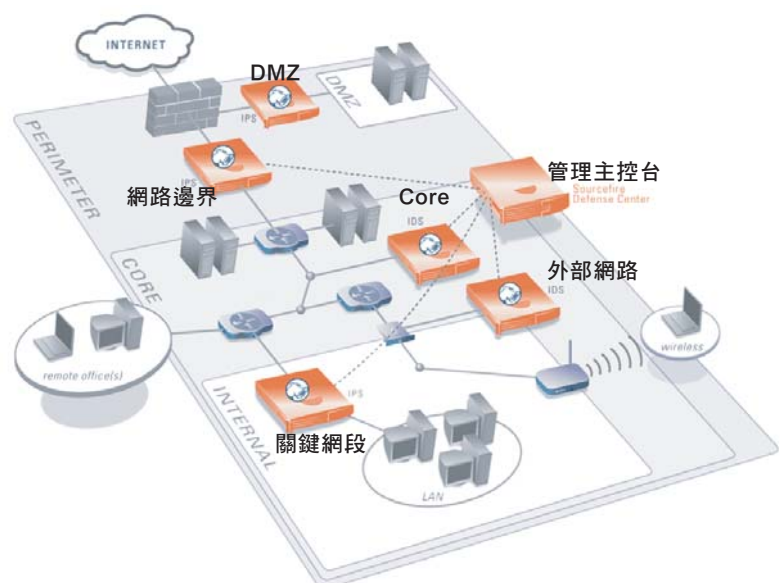
Sourcefire Vulnerability Research Team (VRT) 是一群技術卓越的安全專家所組成，負責維護Snort的防護規則，並且建立Sourcefire IPS解決方案所使用的正式規則。

### • 安全政策一致性

透過上述的資訊，Sourcefire還能做到安全政策控管功能，確保員工及電腦符合企業的安全政策。舉例來說，公司不允許使用即時通訊軟體，當員工的電腦上安裝Skype並進行連線時，就會被Sourcefire偵測到，並立即通知管理人員；另外，如果員工私自使用個人的電腦連線內部網路，一樣會被Sourcefire偵測，並發出警示。

### • 內外部完整防護

新世代的入侵防禦系統，除了部署在閘道端之外，更可部署在資料中心、內部網段、DMZ區，防禦來自內部的攻擊行為。因此，Sourcefire的產品效能從5Mbps至40Gbps，能夠充份滿足企業各種需求，部署在各種節點上，協同防禦每個角落。



所有 Sourcefire 解決方案所提供的威脅偵測範例

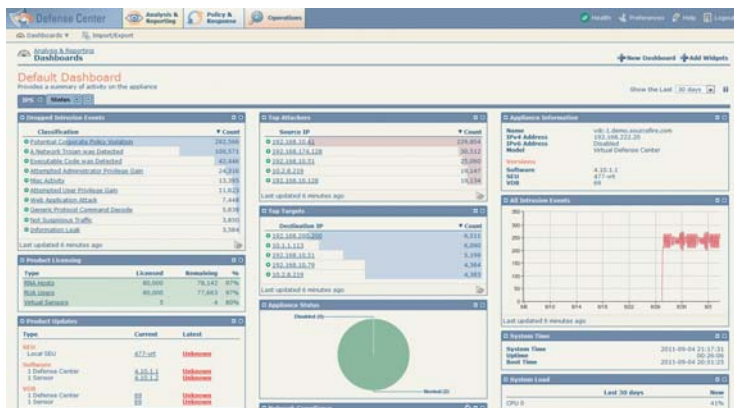
- DoS 攻擊
- 緩衝區溢位
- P2P 攻擊
- 蠕蟲病毒
- 特洛伊木馬病毒
- 後門攻擊
- 間諜軟體
- 無效標頭
- 混合型威脅
- 頻率攻擊
- 零時差威脅
- 連接埠掃描
- VoIP 攻擊
- IPv6 攻擊
- 統計異常
- 通訊協定異常
- 應用程式異常
- 畸形流量
- TCP 劃分及 IP 分段

## • 入侵事件優先等級

透過Sourcefire的入侵事件優先等級，能夠篩選掉95%無威脅風險的事件，只保留5%需要關注的事件，降低管理負擔，對攻擊有漏洞的應用程式，可設定立即提示管理者。某個採用Sourcefire的客戶，其事件數就由2000萬筆減少為2000筆有效事件警示，大幅降低誤判率與減少管理負擔。

## • 關連式分析報表

透過RNA、RUA及入侵事件優先等級等技術，Sourcefire的關連式分析報表，能夠最即時的協助管理者找到問題點。在每一筆日誌，管理者除了能夠查看到攻擊事件、來源/目的IP、使用者、日期…等資訊外，還能知道該主機的作業系統版本、應用程式版本及對應弱點等資訊，讓管理者不需東查西找，在一份報表中就能查到全部所需的資訊。



管理主控台的關聯式分析報表，除了查看完整的攻擊日誌，還提供獨家的RNA及RUA功能，能協助管理者快速排除問題。

## • 與第三方廠商協同防禦

由於Sourcefire具備開放原始碼的彈性，因此能夠快速輕鬆的與各種協力廠商整合，包含弱點管理系統、安全資訊與事件管理系統（SIEM）、網路存取控制（NAC）及網路鑑識等，簡化資安產品部署與規畫程序，讓企業的投資成本獲得最大的效益。

當你每天忙著查看入侵系統的日誌，忙著驗證攻擊是否生效，忙著每個月攻擊分析報表，忙著每季的弱點掃描，忙著…；請暫時停下手邊的工作，聽聽我們介紹Sourcefire新世代入侵防禦系統，它可以協助你減輕很多傳統入侵防禦系統繁雜的日常工作，讓你把時間留著企業的關鍵業務。

## Discover 探索

## Determine 診斷

## Defend 防禦

Sourcefire 3D = 探索 Discover + 診斷 Determine + 防禦 Defend

一般的入侵防禦系統是以特徵資料庫為基礎，為了減輕管理者的負擔，強調只要套用其預設的規則，即可防禦各類攻擊；但換個角度來想，每家公司有不同的網路架構、應用、系統及使用者，加上現今的網路環境隨時隨地都在變動，一條規則根本就無法符合每家公司的需求。

Sourcefire認為，要解決上述的問題，必須先「探索」企業內部有什麼，其獨家的RNA及RUA技術，能夠收集企業內部的各種資訊，員工新安裝的應用程式，或是自行帶來的筆記型電腦，都能在第一時間即時通知管理者。

然後，系統再透過上述的資料進行「診斷」，Sourcefire獨家的自動調校規則技術（Auto Tuning）能夠協助管理者判斷要開啟哪些偵測規則，不但減少管理負擔，也降低防禦空窗期，達到真正有效的「防禦」。舉例來說，A公司只有Windows電腦，就不會啟用針對Mac電腦的防禦規則；如果B公司有Linux伺服器，就會啟用針對Linux系統弱點的防禦規則；若是員工的電腦上被偵測出未安裝修檔，或應用程式仍存在弱點，Sourcefire就會啟用相關的規則，來防禦這台電腦。

最後，管理者能夠在關連式分析報表，檢視整體的防禦效果，而且其日誌數量是傳統入侵偵測系統的5%。讓你只關注需要關注的事件。

## Sourcefire 規格

| 機型     | 3D2000         | 3D2100  | 3D2500                         | 3D3500 | 3D4500 | 3D6500                         |
|--------|----------------|---------|--------------------------------|--------|--------|--------------------------------|
| IPS 效能 | 100Mbps        | 250Mbps | 500Mbps                        | 1Gbps  | 2Gbps  | 4Gbps                          |
| 網路介面   | 4 Copper 1Gbps |         | 8 Copper 1Gbps                 |        |        | 12 Copper 1Gbps                |
|        |                |         |                                |        |        | 6 Copper 1Gbps + 4 Fiber 1Gbps |
|        |                |         | 4 Copper 1Gbps + 4 Fiber 1Gbps |        |        | 6 Copper 1Gbps + 2 SR/LR       |
|        |                |         |                                |        |        | 10Gbps                         |
|        |                |         | 4 SR/LR 10Gbps                 |        |        |                                |
| 記憶體    | 1GB            | 1GB     | 2GB                            | 4GB    | 8GB    | 16GB                           |
| 磁碟空間   | 40GB           | 160GB   | 160GB                          | 160GB  | 160GB  | 160GB                          |
| 外型     | 桌上或機架          | 1U      | 1U                             | 1U     | 1U     | 2U                             |

| 機型     | 3D8140         | 3D8250         | 3D8260         |
|--------|----------------|----------------|----------------|
| IPS 效能 | 6Gbps          | 10Gbps         | 20Gbps         |
| 設備效能   | 10Gbps         | 20Gbps         | 40Gbps         |
| 模組化介面  | 最多 3 組         | 最多 7 組         | 最多 6 組         |
| 網路模組   | 4 Copper 1Gbps | 4 Copper 1Gbps | 4 Copper 1Gbps |
|        | 4 Fiber 1Gbps  | 4 Fiber 1Gbps  | 4 Fiber 1Gbps  |
|        | 2 SR 10Gbps    | 2 SR 10Gbps    | 2 SR 10Gbps    |
|        | 2 LR 10Gbps    | 2 LR 10Gbps    | 2 LR 10Gbps    |
| 記憶體    | 24GB           | 48GB           | 96GB           |
| 支援堆疊   | 是              | 是              | 否              |
| 機器     | 1U             | 2U             | 4U             |

| 管理主控台            | DC750  | DC1500  | DC3500   |
|------------------|--|---------|----------|
| 最大受管理 IPS 數      | 10   | 35      | 150      |
| 最大 IPS 事件儲存數     | 2000 萬筆  | 3000 萬筆 | 15000 萬筆 |
| 最大 IPS 事件接收率 (秒) | 2000   | 6000    | 10000    |
| 最大 Flow 資料率 (秒)  | 2000   | 6000    | 10000    |
| 記憶體              | 2GB  | 6GB     | 12GB     |
| 事件儲存空間           | 100GB  | 125GB   | 400GB    |
| 雙電源              | 否  | 否       | 是        |
| 備註               | RNA、RUA 及關連式報表需搭 Sourcefire 管理主控台 Defense Center |         |          |

## Sourcefire 簡介

- 2001年由Snort的開發者Martin Roesch所成立，並擔任公司的技術長
- 目前全球有2300多家客戶，客戶群包含各行各業，如美國政府、科技大廠
- 2006~2010年：Gartner IPS報告，位於領導者象限
- 2009~2010年：NSS Labs IPS測試評比第一名，獲選為最佳偵測系統
- 獲得SC Magazine評選為最佳IDS/IPS
- 獲得ICSA Labs認證



**NetFOS**  
逸盈科技

Sourcefire 新世代 IPS 解決方案  
逸盈科技股份有限公司

台北 (02) 6636-8889 新竹 (03) 623-5588  
台中 (04) 3606-8999 高雄 (07) 862-8889