威脅檢測與回應

關聯、優先、回應

網路犯罪份子正在準備日益增長的複雜性攻擊，使用協同方式從任何地方與連接來訪問您的網路。安全防護措施必須跟上時代的步伐，透過添加在網路和端點的檢測能力，以及有能力對事件活動關聯到有針對性的行動。WatchGuard 的威脅檢測和回應（TDR：Threat Detection and Response）服務相關的網路和端點安全事件與威脅智能檢測，確定優先等級並立即採取行動阻止惡意軟體攻擊。TDR 能使中小型企業和託管安全服務提供商（MSSP）能夠在關鍵業務數據或組織生產力受到威脅之前自信的補救高級惡意軟體攻擊。

網路和端點事件關聯

ThreatSync 是 WatchGuard 新基於雲關聯和威脅的評分引擎，提高整個網路到端點的安全意識和回應。ThreatSync 從 WatchGuard Firebox 上收集事件數據，並關聯 WatchGuard 主機傳感器和雲威脅情報的數據，以生成一個全面的威脅分數來指導補救。

企業級威脅情報

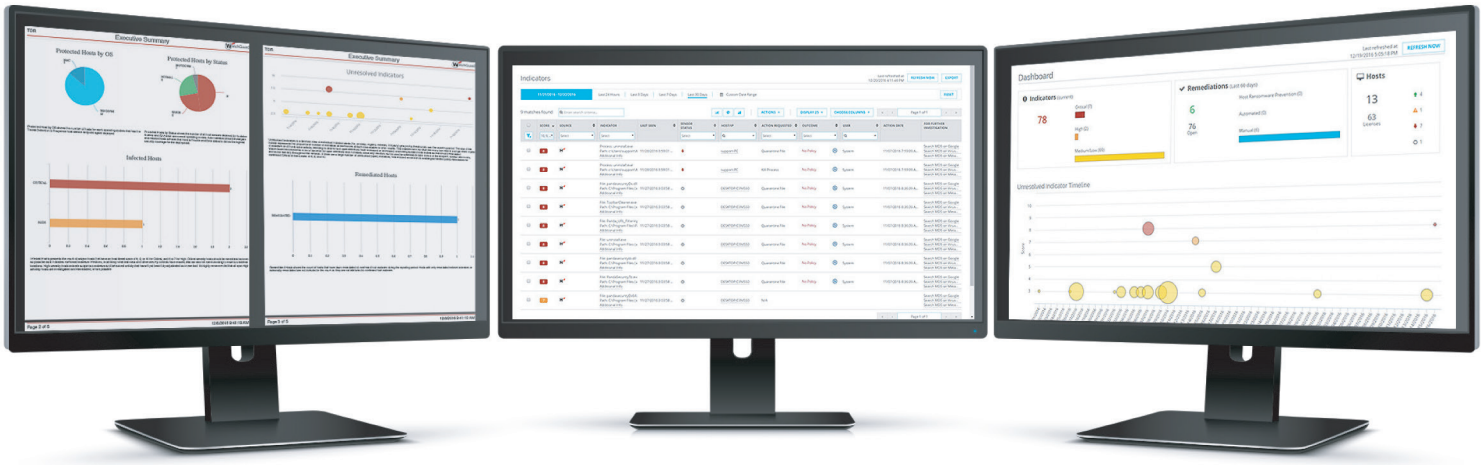
第三方供應商的雲情報威脅智能感知系統以前只提供給較大預算和更大的安全團隊與企業組織受益。利用威脅檢測和回應，WatchGuard 可以整合和分析威脅情報 - 提供安全優勢，而不會增加相關的複雜性或成本。

擴展端點的可視性

輕量級的 WatchGuard 主機傳感器只佔少量硬體資源即可監控和檢測設備上的威脅活動。主機傳感器持續地將這些事件發送到 ThreatSync 進行關聯和評分，接收並執行戰術補救指令。主機傳感器透過雲做集中管理，使託管安全服務提供商和 IT 管理員能夠輕鬆的在世界任何地方部署、更新和管理主機傳感器。

先進的勒索軟體預防

主機勒索軟體防護（HRP：Host Ransomware Prevention）是 WatchGuard 主機傳感器內勒索軟體的特定模塊。HRP 利用行為分析引擎和誘騙目錄來監控一系列廣泛的特性，以確定給定的操作是否與勒索軟體攻擊相關聯。如果威脅是惡意的，HRP 可以在端點上的文件加密之前自動防止勒索軟體攻擊。



台灣銷售代表：Jacky Wu 吳東信 • 聯絡電話：0955-707-006 • Web：www.watchguard.com

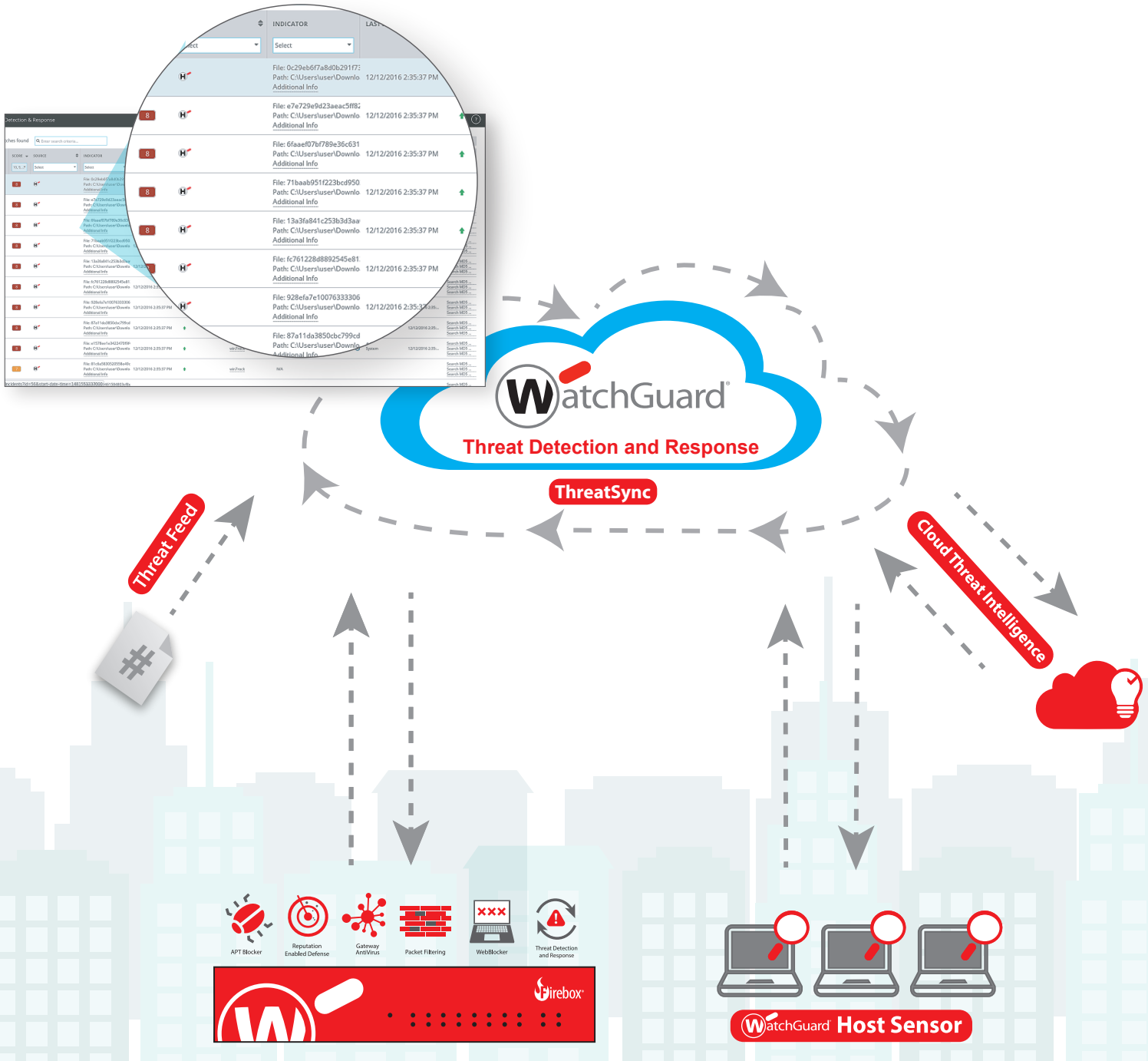
提高安全性與關聯性

ThreatSync，TDR 的基於雲計算關聯性和威脅評分引擎，提高了網路對終端的安全意識和回應。

ThreatSync 可以在 Firebox 的其他幾個安全服務，包括 APT 攔截器、信譽防護（RED）、閘道防毒和網站攔截器來收集網路事件數據。這些事件都通過 WatchGuard 的主機傳感器和企業級的威脅智能感知系統檢測到威脅相關活動。

ThreatSync 接著分析這一威脅的數據提供了全面性的威脅分數和整體嚴重程度的排名。特定回應操作將被傳輸回主機傳感器，包括隔離文件、刪除過程或刪除註冊表值。

這種專有技術不僅透過提高對網路和端點上威脅的可視性來減少檢測時間，並且最終透過生成全面性的威脅分數來確認回應，進而提高補救時間。



單一設備，單一包裝，完整安全

威脅檢測和回應，可透過 WatchGuard 的完整安全套件來提供，其中也包括像 APT 攔截器、網站攔截器、閘道防毒、入侵防護服務和信譽防護等高級安全解決方案。

雖然每個安全解決方案都可以防禦高級威脅，但當安全防禦協同工作時，用戶可以獲得最大的利益，提供最強的安全保護和最高效率，而不會影響 Firebox 的性能。

產品	標準安全套件	完整安全套件	基礎安全套件
防火牆 Stateful Firewall	✓	✓	✓
行動裝置 VPN	✓	✓	✓
分公司 VPN	✓	✓	✓
應用代理 Application Proxies	✓	✓	✓
入侵防護（IPS）		✓	✓
應用程式控制（App Control）		✓	✓
網站攔截器（WebBlocker）		✓	✓
反垃圾郵件（spamBlocker）		✓	✓
閘道防毒（GAV）		✓	✓
信譽防護（RED）		✓	✓
網路探索（Network Discovery）		✓	✓
進階持續性滲透攻擊攔截（APT）		✓	
數據外洩服務（DLP）		✓	
Dimension Command		✓	
威脅檢測與回應（TDR）		✓	
支援	標準（24x7）	金質（24x7）	標準（24x7）

Firebox 型號	包含主機傳感器（Host Sensors）
T10	5
T30	20
T50	35
T70 / M200	60
M300	150
M400 / M440 / M500 / M4600 / M5600	250
FireboxV S	50
FireboxV M	250
FireboxV L	250
FireboxV XL	250

需要更多主機傳感器？

威脅檢測和回應包括基於您的 Firebox M 系列、T 系列或 FireboxV 設備中內建一定數量的主機傳感器。 並可根據需求，通過升級產品提供其他主機傳感器的數量。

Host Sensor 主機傳感器加購選項
10 Host Sensors
25 Host Sensors
50 Host Sensors
100 Host Sensors
250 Host Sensors
500 Host Sensors

威脅檢測和回應包括基於設備型號中內建一定數量的主機傳感器。可以加購其他主機傳感器，並添加到帳戶可用的總體主機傳感器數量中。

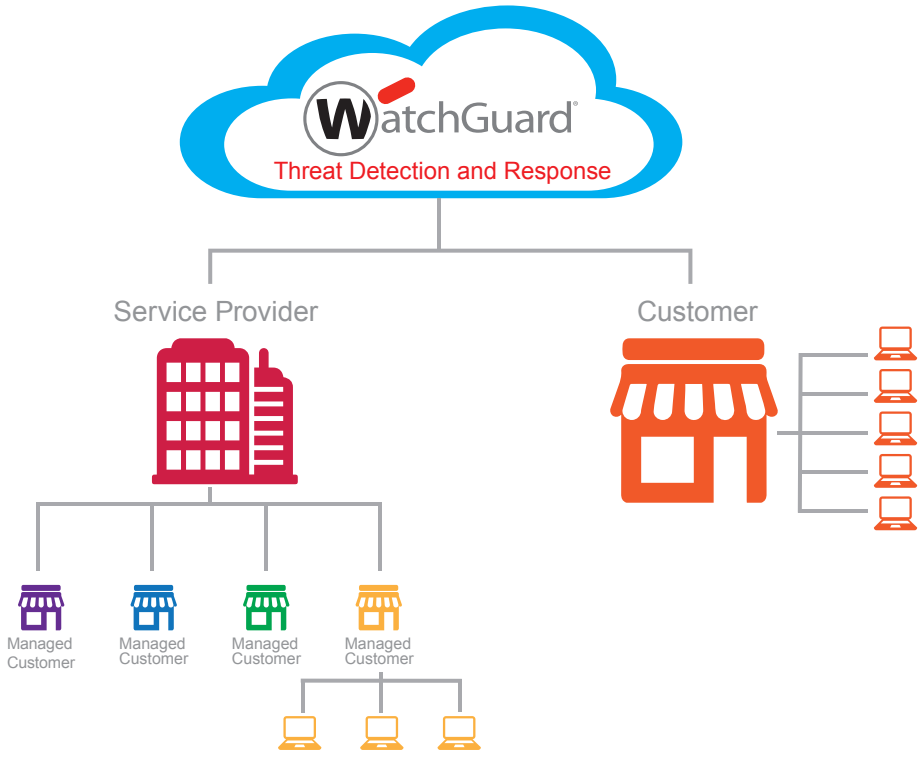
威脅檢測與回應

可管理，可擴展的安全性

威脅檢測和回應能使用戶能夠輕鬆地擴展和管理他們的安全性。基於雲的服務，便於管理員和操作員迅速在整個組織中部署主機傳感器，創建策略並進行一鍵修復。

TDR 可以輕鬆擴展，並使您的業務增長。雖然每個 TDR 實例都包含基於現有設備一定數量的主機傳感器，但升級包可以輕鬆添加更多主機傳感器以滿足您的組織需求。

如果管理安全服務不是貴組織寶貴時間和資源的最佳選擇，我們廣泛的 MSSP 合作夥伴網路使您能夠在處理日常操作時利用到威脅檢測和回應的優勢。



了解更多有關威脅檢測和回應的詳細信息。有關 WatchGuard 最新安全服務的更多信息，請訪問我們的網站：**www.watchguard.com/TDR**

如何開始

WatchGuard 擁有業界最大的加值經銷商和服務提供商網路。要開始使用，請訪問我們的網站找到最好的合作夥伴業務，或選擇直接與我們聯繫，我們會回答您的任何問題，並幫助使您的需求提供完美的合作夥伴。

- 請訪問我們的“查找經銷商”頁面，找到您附近的合作夥伴：**http://findpartner.watchguard.com**
- 與 WatchGuard 安全專家交談：**www.watchguard.com/wgrd-sales/emailus**

關於 WatchGuard

WatchGuard® Technologies, Inc. 是全球超過 75,000 家客戶的網路安全、安全 Wi-Fi 和網路智能產品和服務的全球領導者。公司的使命是通過簡單易用的方式為所有類型和規模的公司提供企業級安全性，使 WatchGuard 成為分佈式企業和中小型企業的理想解決方案。WatchGuard 總部位於華盛頓州西雅圖，在北美、歐洲、亞太和拉丁美洲設有辦事處。要了解更多信息，請訪問 **watchguard.com**