奧義智慧科技
Powered by CyCraft

THREAT WALL

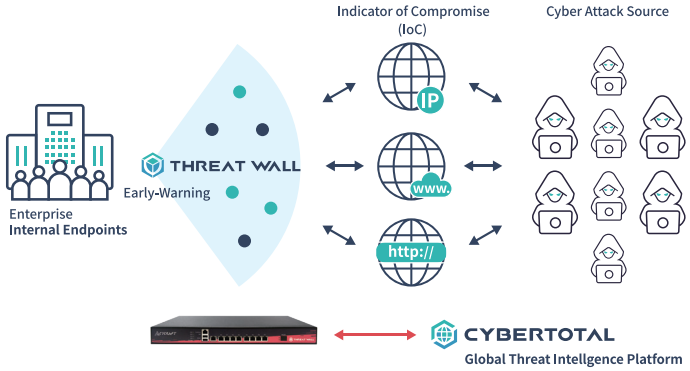
Network Detection & Response ThreatWall 產品規格書

基於 FAST 精神的 NDR

- **快速 Fast**：無論系統規模大小皆維持 Inline 高效處理運算。
- **精準 Accurate**：每小時自動化更新最新惡意網域、IP 位址情資。
- **簡潔 Simple**：可於數分鐘內完成部署，中控介面簡單易操作。
- **全貌 Thorough**：超前部署，徹底阻絕可疑網路威脅。

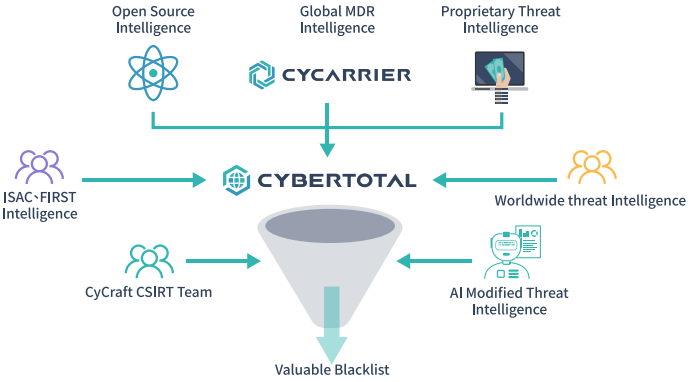
ThreatWall 主要功能

- 採用奧義智慧獨家 AI 主動式惡意網域偵測引擎，有效阻擋新型態網路威脅及零時差攻擊。
- 整合奧義全球威脅情資平台，每小時動態更新最新阻擋規則。
- 提供 Inline 阻斷及 Mirror 模式彈性架構，部署於企業防禦最前線，大量減輕後端資安設備處理負擔。
- 相容 DNS Response Policy Zone (RPZ)，有效防止惡意 DNS 查詢。
- 無須 SSL 解密金鑰即可因應相關的網路威脅。
- 產出合規阻擋報表，可對應各國家資安資訊分享與分析中心 (ISAC) 機構發布之情資列表，如F-ISAC等。



ThreatWall 運作流程

每當出現新型態的惡意程式、網路釣魚、APT 中繼站等可疑連線時，ThreatWall 將扮演外圍第一道防線，阻擋潛在威脅進入企業網路。藉由與 CyberTotal 全球威脅情資平台的整合，ThreatWall 提供有效且快速的偵測與阻擋系統，利用具脈絡的威脅資訊，使系統收集的入侵指標 (Indicator of Compromise, IoC) 更加豐富，用以檢查每個目標 IP 位址、網域與網址。ThreatWall 可即時呈現單位內所有攔阻紀錄，了解相關惡意行為證據、多家情資廠商針對攔阻標的之信譽評等，以及單位內發掘的惡意流量與其對應 IP 之地理位址和國別等。

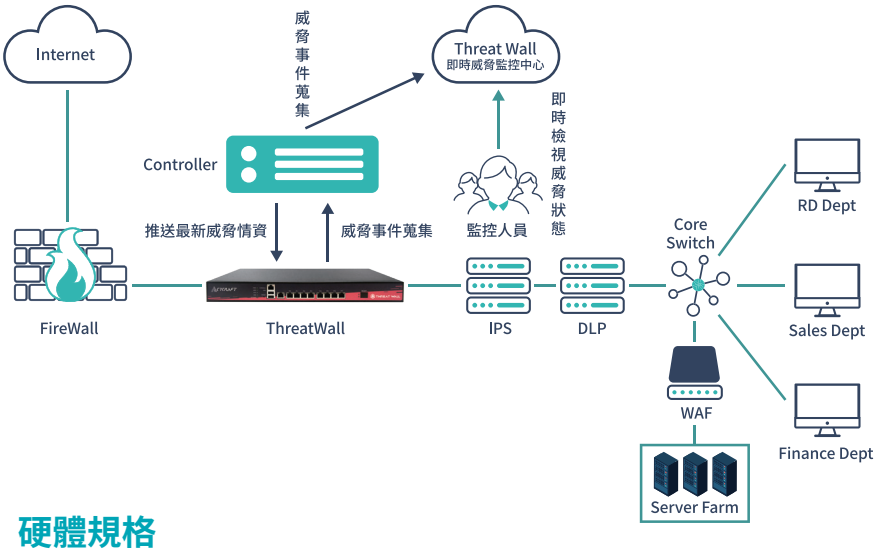


ThreatWall 高含量情資產製流程

傳統的威脅情資 (Cyber Threat Intelligence, CTI) 通常以交換靜態的黑名單為主，包含 IP 位址、網域與 MD5 等，普遍缺乏針對更高層級攻擊者與攻擊方式的情資。而 ThreatWall 使用 CyberTotal 威脅情資，以 AI 技術即時彙整與解析逾 130 國的威脅樣態，可主動防禦全球首次發現的新型態可疑連線及零時差攻擊，並即時分析全球攻擊樣態，轉換成最新阻擋規則。ThreatWall 支援高達五千萬條阻擋規則，可阻絕各種網路威脅，包含釣魚網站、殭屍電腦、APT 惡意程式、Banking Trojan 等。

ThreatWall 關鍵優勢

- 內建 DNS 防禦，支援 Domain 類型黑名單，較傳統僅針對 IP 的黑名單系統更為精準，大幅降低誤判率並避免疲勞告警。結合 DNS RPZ 防禦概念，節省企業額外建置 RPZ 設備之成本。
- 整合 CyberTotal 全球威脅情資平台，情資數量及品質皆領先於業界。結合情資資料庫與 AI 自動化分析，提供業界最詳盡完整的阻擋原因分析及惡意行為資訊。
- AI 即時解析並動態更新阻擋規則，可精準偵測及擋下新型態可疑連線，達到真正的主動防禦、阻絕零時差攻擊。
- 提供 API 及 CSV 下載功能，方便與其他資安平台進行整合，ThreatWall 由臺灣團隊研發，可依據客戶需求彈性客製。



部署架構

ThreatWall 支援 Inline 及 Mirror 彈性部署架構，建議部署於防禦前端，可消除網路威脅、避免惡意流量進入單位內部，造成資安防禦設備負擔過重。

硬體規格

	ThreatWall 1G	ThreatWall 10G	ThreatWall 10G20
網路介面 Network	1G RJ45*8	10G SFP+*2 1G RJ45*8	10G SFP+*20 40G QSFP*2+10G*12 40G QSFP*4+10G*4
管理介面 Management Interface	1G RJ45*1	1G RJ45*1	1G RJ45*1
數據格式 Data Format	Ethernet PCAP File	Ethernet PCAP File	Ethernet
儲存 Storage	SATA2*1	SATA2*2	2GB (virtual disk)
黑名單容量 Indicator Capacity	500 萬 IoCs	2,000 萬 IoCs	5,000 萬 IoCs
電源 Power	AC 110V-220V input	AC 110V-220V input	Dual AC 110V-220V input

關於奧義智慧

世界領先 AI 資安公司，以創新 AI 技術自動化資安防護，內建 EDR、CTI、NGAV、NDR 整合新一代 AI 資安戰情中心，獲得逾五十個政府機關、警政、國防單位，以及三成金融機構、數十家關鍵領域龍頭企業的信賴，市占率國內第一。2020 年美國 MITRE ATT&CK® 公開評測最佳偵測能力，臺灣新創唯一入選全球資安產業地圖。從端點到網路、從調查到阻擋、從自建到託管，CyCraft AIR 提供客戶主動防禦，全方面守護企業安全。

MITRE | ATT&CK® Evaluations

Momentum CYBER
CYBER SCAPE

Interop BEST OF SHOW AWARD 2020