

MITRE | ATT&CK® Evaluations Enterprise 2025

全球唯一 連續 3 年以預設配置 100% 達標

Endpoint Security / Network Security
User & Identity Protection
Mobile Protection / Email Security
Cloud Security / SaaS Security

It's ALL I Need!

Cynet All-in-One Security Platform 是以 EDR 為核心，整合端點、身分、電子郵件、網路、雲端、SaaS、行動裝置、自動化應變與免費 24/7 MDR 服務的進階資安防護平台。透過單一平台深度分析各類進階威脅並提供原生自動化回應能力，Cynet 可協助企業大幅降低因多套資安工具並行而造成的部署複雜度、告警分散與維運負擔，更有利於資安團隊快速掌握威脅脈絡並採取行動。

MITRE | ATT&CK® Evaluations Enterprise 2025 測試範圍延伸至雲端環境與多平台攻擊情境，以反映現代攻擊跨端點、身分、網路與雲端環境移動的實際風險。Cynet 是參與評測之眾多資安大廠中，唯一以預設配置未進行任何變更即達成 100% Protection、100% Detection Visibility、100% Technique-Level Coverage 與 0 Detection False Positives 之成果，充分證明其在攻擊偵測、威脅防護與跨環境可視性方面的即時性與精準度。

現代攻擊已不再是單一事件，而是從釣魚郵件、帳號濫用、憑證竊取、端點入侵、橫向移動到勒索軟體部署等多個階段串連而成。Cynet 之核心價值在於將原本分散於不同資安工具中的訊號整合至同一平台，結合其 CyOps 與 CyAI 原生 AI 關聯分析能力，將 email、identity、endpoint、network、cloud 與 SaaS 等訊號整合為完整攻擊路徑分析，協助資安團隊避免僅看到孤立告警，而能依據企業預先授權與平台支援範圍，執行威脅調查、指標搜尋、受影響資產定位、端點隔離、惡意程序終止、阻擋網路連線與事件修復等措施，在威脅橫向移動、勒索軟體部署或事件擴大前進行快速遏止。

Free!

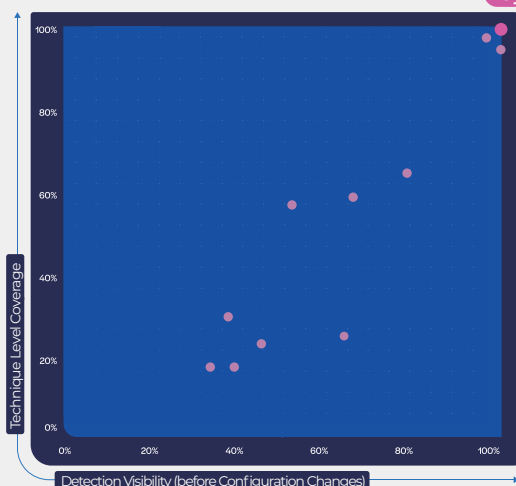
CYOPS

AI-Powered 24x7 MDR with Extended SOC, Proactive Threat Analysts & Lighthouse Credential Monitoring

CYAI

AI-Powered Detection, Automation, and Response Natively Built into the Core of Cynet

MITRE | ATT&CK® 2025 Evaluations Results Cynet



CyOps 是 Cynet All-in-One 與 Elite 服務方案所提供的免費 24/7 Proactive MDR (Managed Detection and Response，託管式偵測與回應) 與 Extended SOC 服務，結合其全球資安分析師、威脅獵捕專家、事件應變團隊與 CyAI 原生分析能力，協助企業全天候監控、分析並應對各類進階資安威脅。企業即使沒有完整 SOC 團隊，亦能取

得持續性的威脅監控、事件分析與應變支援。CyOps可協助偵測勒索軟體、惡意程式感染、帳號入侵、異常登入、橫向移動、可疑 PowerShell / WMIC行為、異常網路連線、端點異常活動與零時差攻擊等威脅，降低企業因資安人力不足而延誤判斷與處置的風險。

CyOps可搭配Cynet 原生 SOAR 與自動化事件回應能力，協助企業執行或建議端點隔離、惡意程序終止、阻擋網路連線、清除惡意檔案、停用帳號、強制重新驗證或其他補救措施，藉此縮短 MTTD 與 MTTR，降低資安事件擴散、橫向移動與勒索軟體部署風險。

CyOps的價值不只是「代管監控」，更在於與CyAI 形成持續回饋迴圈。CyAI 協助處理大量告警關聯、攻擊路徑辨識與自動化初步應變；CyOps 專家則針對高風險事件進行驗證、調查與專業判斷，並將實際事件經驗回饋至偵測邏輯與模型優化中，使平台能持續提升偵測精準度與應變效率。

About Cynet

Cynet 2015年創立於以色列，服務據點遍布美國、加拿大、以色列、亞洲等逾十多個城市，並已成功服務全球數千家金融、醫療、製造、教育等各規模/產業之客戶。

現今市場中的資安應用與架構往往過於複雜且所費不貲，Cynet 的願景是讓全球不論規模大小或資源多寡的企業組織，特別是SME中小型企業，皆能與 Fortune 1000 大型企業同樣享有信任無虞、更容易取得、更具成本效益的資安防護服務，協助客戶遠離資安風險而更能專注實現其組織的熱情、目標與使命。

2026 GigaOm XDR Radar 報告中，Cynet 亦被評為「Leader (領導者)」與「Outperformer (表現卓越者)」，GigaOm將Cynet定位於「Innovation / Platform Play (創新 / 平台型解決方案)」象限，肯定其平台完整性，以及在威脅生命週期自動化方面的快速創新能力。

Cynet All-in-One 進階資安防護服務方案

- Platform 管控平台 (地端 或 雲端)
- Endpoint Detection and Response (EDR)
- Endpoint Security Posture Management (ESPM)
- Mobile Threat Detection (MTD) *選購
- Network Detection and Response (NDR)
- User Behavior Analytics (UBA)
- Deception
- Email Security
- SaaS & Cloud Security Posture Management (SSPM & CSPM) *選購
- Centralized Log Management (CLM) & Open XDR *選購
- Orchestration
- Services / MDR / Threat Intel

Compliance

SOC 2 Type II

符合 SOC 2 之安全性、可用性與機密性信任服務準則 (TSC)，確保內部基礎設施、控制機制及客戶資料的最高資安標準。

ISO 27001

遵循全球公認的資訊安全管理標準 ISO 27001，將資訊安全、資料隱私與持續改進整合至日常營運中，致力於保護資訊、有效管理風險並遵守全球資安標準。

PCI DSS

以有效且具高CP值的方式遵循 PCI DSS 的第 5、6、10 和11項規範，確保信用卡資訊的安全儲存與傳輸。

HIPAA

支援醫療組織遵循HIPAA八大類別規範，保障個人健康資訊的安全與隱私。

NIST CSF

符合NIST網路安全框架的五大核心功能：識別、保護、偵測、回應與恢復，提升關鍵基礎設施之資訊安全。

CMMC

協助與美國國防部供應鏈相關之公司達成CMMC 2.0計畫中的高標準規範，確保其資訊安全成熟度符合國防產業的需求。

GDPR (歐盟與英國)

遵守歐盟與英國的通用資料保護規範(GDPR)，確保個人資料的正確處理與保護。

