BlackBerry | Cybersecurity

# 基於AI的端點偵測與回應

## CylancePROTECT®

CylancePROTECT® 是基於本地Cylance AI的端點防護平台(EPP)，協助即時偵測、阻擋與控制端點裝置處理各式進階複雜網路攻擊。

CylancePROTECT® 無需事先經由人工政策設定、連網更新特徵碼、經驗演算法(Heuristics)或傳統沙箱，適合特殊場域運行，有效降低人力介入之維運成本。

## CylanceOPTICS®

CylanceOPTICS® 是基於雲端架構的端點偵測與回應服務(EDR)，可與CylancePROTECT®搭配使用，有效協助預防與發現組織內所有裝置的網路威脅。

CylanceOPTICS® 採用「Prevention First」的方式，可在數毫秒之內發現並採取行動來防止網路攻擊進一步發展，有效消除延遲回應造成的損失。

## CylancePROTECT® 特色

### 基於Cylance AI的惡意軟體防護

- 有效偵測所有已知或未知的惡意軟體與zero-day payloads，可在攻擊發動前進行封鎖。
- 自動發現可疑的記憶體使用情形(例：無檔案攻擊)，立刻回應。

### 輕量級的端點Agent

- 與傳統防毒軟體相比，僅需佔用少量的CPU資源。
- 完全本地AI能力，無需基於特徵碼或雲端運算。

### 全面可視化Dashboard

- 控制可連入特定系統的裝置白名單、可根據類別設定存取權。
- 即時中斷應用程序，隔離受駭端點裝置，避免威脅擴散。
- 自定義使用者角色和權限。

## CylanceOPTICS®特色

### 快速偵測並回應勒索軟體

- CylanceOPTICS®結合CylancePROTECT®，能即刻偵測並且自動回應威脅，不需花費數小時或數天。
- 基於Cylance AI分析，人工介入的占比更少

### 透過機器學習預防廣泛的安全事件

- CylanceOPTICS®從端點偵測與收集所有威脅動作，大幅減少攻擊面與威脅橫向擴張的可能性。
- 全面覆蓋攻擊鏈進程，將網路攻擊可視化。

### 自定義自動回應

- CylanceOPTICS®可藉由自訂與內建的腳本，自動化回應並處理端點威脅。

## 適用情境

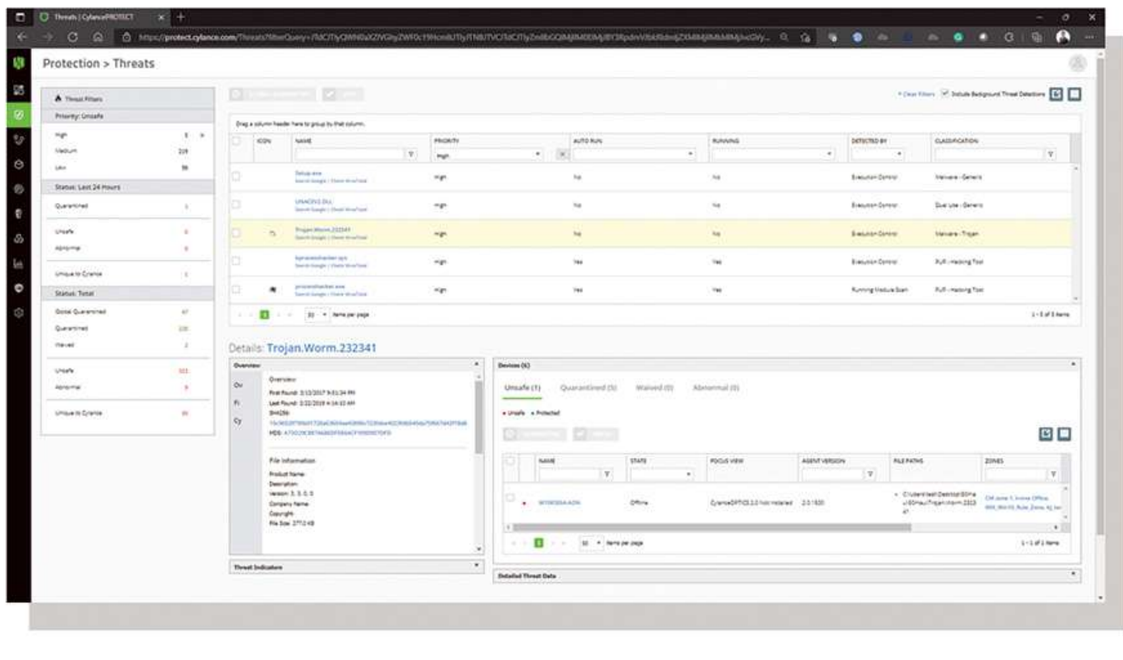
- 適用管制連網之特殊場域
  EX：軍警單位，高科技產業等。
- 適用OT等特殊作業系統等異質平台環境。
- 欲加強防護zero-day與勒索病毒等進階攻擊者。
- 欲補強端點防護管制與安控，有效降低人力事件處理成本者。
- 避免傳統SOC僅監控閘道端之盲區，補強端點監控，強化IR事件調查應變(Incident Response)效益。

## Cylance Protect Mobile

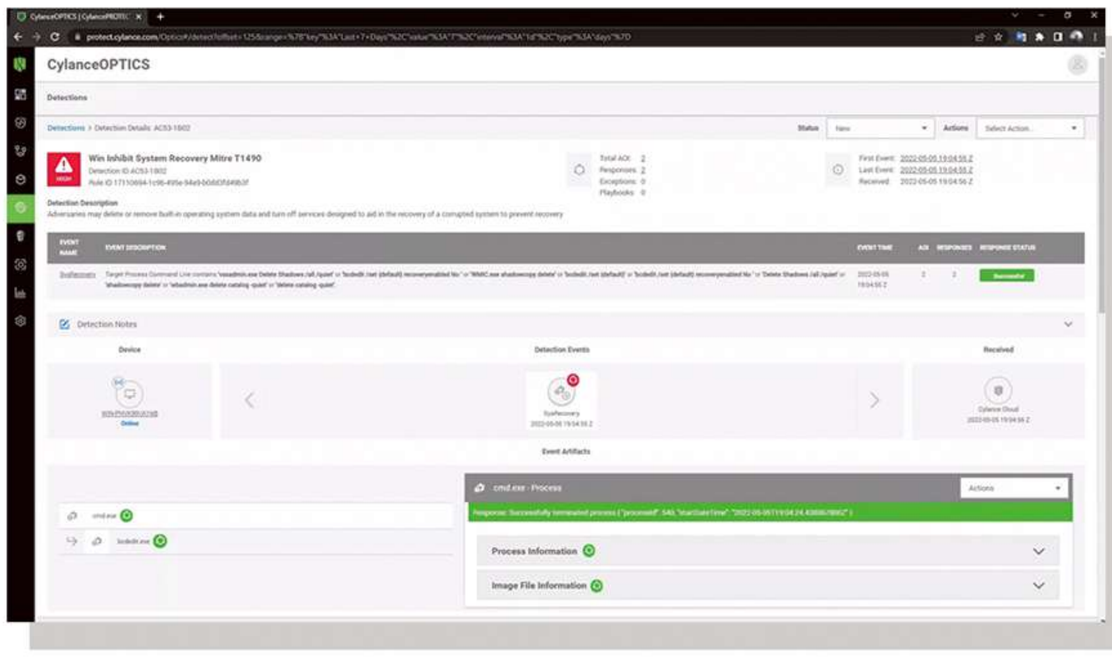
Cylance Protect® 針對手機等行動裝置，推出Cylance Protect Mobile App，協助您隨時監控移動裝置及其應用程式之惡意軟體攻擊。

*功能特點：*

- 網址掃描：防止簡訊釣魚，組止透過惡意SMS/MMS訊息嘗試進行社交工程攻擊的威脅。
- 單一主控平台：行動裝置與主機型電腦終端統一管理與報告。
- 可透過QR Code註冊與啟用。
- 直覺式介面反應裝置健康狀況。
- 提供簡版裝置安全性評估。


Cylance Protect®介面




Cylance Optics®介面

台灣代理商：ACE Pacific Group 鼎峰亞太
業務洽詢 / sales@ace-pac.com
服務專線 / 02-2579-6218
地址 / 台北市松山區敦化南路一段7號10樓