

AhnLab

ENDPOINT PLUS

新世代端點安全防護解決方案

整合防毒、修補、控管、EDR 的統一管理平台 **地端版**



台灣總代理 | 湛揚科技

www.t-tech.com.tw

現代網路威脅正以前所未有的速度演變

攻擊者不斷改進戰術以規避傳統防禦措施。人工智慧驅動的攻擊演化速度比人類防禦者的反應速度更快。在這種快速演變的威脅情況下，您需要的不僅是解決方案，更需要一個面向未來的合作夥伴。結合具深度洞察的威脅情報與人工智慧驅動的防禦系統，主動阻斷威脅。

關於AhnLab

AhnLab成立於30年前，是亞洲領先的資訊安全廠商，擁有超過20年的自主研發經驗。公司專注於端點防護、網路防禦及雲端資安整合管理，其核心技術基於自主開發的威脅偵測引擎和AI分析平臺，強調即時應對在地威脅、低誤報率與高準確率，以及可擴充的防禦架構，為企業提供從防護、偵測到回應的一站式解決方案。

AhnLab長期服務於金融、製造、電信、醫療及公共事業等多元領域，提供穩定、可擴充且符合法規要求的整體資安策略。該公司是Gartner認證的亞太區指標性資安廠商之一，也是韓國最大資安公司，總部位於首爾，客戶包括全球《財星》500大企業。

AhnLab提供OT/IT全方位安全解決方案，服務範圍遍及全球。其OT安全旗艦產品AhnLab CPS PLUS涵蓋EPS、ICM、MDS和Xscanner等。此外，AhnLab的端點安全產品如EPP、V3、EDC和EPrM等多次獲得國際評測機構的認證，並被Gartner列為亞太區領先的代表性廠商。值得一提的是，AhnLab於2025年授權湛揚科技為臺灣區代理商。

Why Customers Trust AhnLab



逾30年的專業經驗與卓越技術

在網路安全行業的領先地位，擁有無與倫比的技術深度。



世界級的威脅情報

提供可操作的威脅情報，能夠預測未來攻擊。



全面保障

為您的數位基礎設施各個方面提供端到端的安全生態系統。

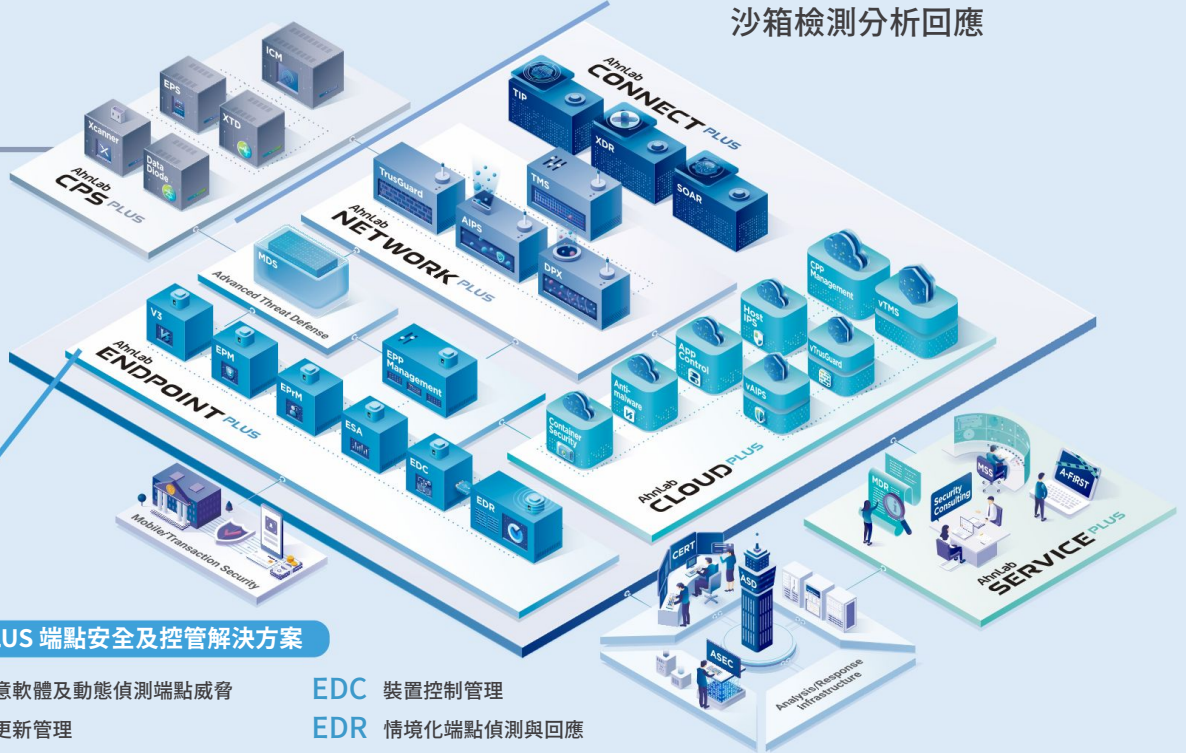


AhnLab Security Map

CPS PLUS 工業控制系統專用安全解決方案

- EPS 工控專用系統的輕量級代理程式
- Xscanner 免安裝式掃毒工具，快速檢測惡意威脅
- Data Diode 單向資料閘道，實現物理隔離與資訊只出不進的高安全傳輸

MDS 針對未知威脅進行全面即時沙箱檢測分析回應



Endpoint PLUS 端點安全及控管解決方案

- V3 防惡意軟體及動態偵測端點威脅
- EPM 軟體更新管理
- EPrM 個人隱私資訊控管
- EDC 裝置控制管理
- EDR 情境化端點偵測與回應

超過30年的網路安全卓越經驗

作為全球歷史最悠久的網路安全公司之一，AhnLab累積了超過30年的前線實戰經驗和經得起驗證的專業實力。從處理國家級安全漏洞到主導關鍵法證調查，我們在長年第一線防禦中，不斷淬鍊出今天的能力。在迅速變化的網路安全產業中，這三十年不只是資歷，更是久經考驗的技術、獨到的威脅情報，以及無可取代的信任紀錄。憑藉這些累積，AhnLab在全球重要的安全評估中持續表現優異；我們通過認證的技術與可靠的解決方案，已為各行各業、遍布多國的客戶提供完善的安全防護。



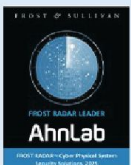
MITRE ATT&CK® 評估

在第七輪評測中，在防護領域實現100%攔截率，充分證明了AhnLab擁有全球領先的安全防護能力。



弗羅斯特沙利文最佳實踐獎

榮獲「韓國年度最佳終端安全公司」稱號連續6年(2019-2024年)。



Frost Radar™ 2025 CPS 安全領導者

被公認為CPS安全解決方案領域的領導者在CPS安全廠商中，創新指數排名第一。



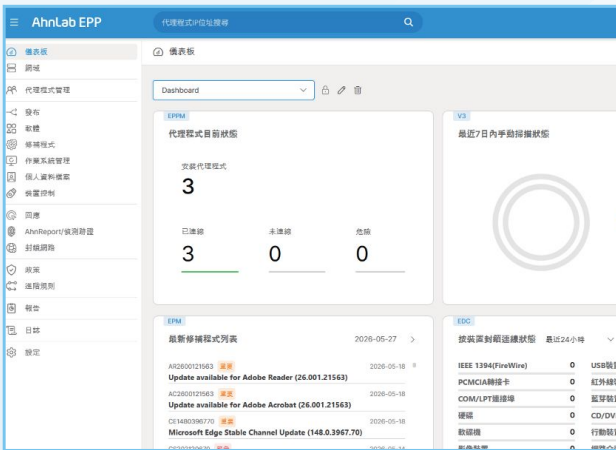
2025 年 AV-TEST 獎項

AhnLab V3 在 AV-TEST 評估中榮獲「頂級產品」稱號，在檢測、效能和可用性標準中均獲得滿分。

AhnLab Endpoint PLUS 單一代理程式，一站式端點防護

關於 AhnLab EPP

AhnLab EPP 以單一代理程式搭配集中管理平台，讓企業可以在同一介面上完成端點防毒、弱點修補與政策管理。管理者能快速掌握整體端點狀態，並依需求啟用個資偵測保護，以及 EDR 等進階防護能力。



【營運效率】單一視窗，集中控管所有端點

以單一管理主控台集中處理防毒、軟體更新、裝置控制、個資保護與 EDR 等多種端點任務，降低分散管理的複雜度。透過可自訂 Dashboard 與整合報表，管理者能在同一畫面檢視風險、政策與合規狀態，決策更快、更有依據。



【快速回應】自動聯防，落實端點資安政策

偵測到異常時依聯動規則自動觸發掃描、封鎖與權限收緊，讓端點在既定資安政策下快速回到安全狀態。



【簡化部署】單一代理，部署管理更省力

以單一代理派送與啟用各項防護模組，並可自訂派送核准的第三方軟體，降低安裝與維護成本。



AhnLab 單一代理程式

「從預防、偵測、評估到修復，AhnLab EPP 提供 360 度無死角的資安閉環。」

🔍 AhnLab EPP 兼顧可視性與治理控管

以聯動規則落實政策一致性，自動化端點事件處理。主動針對端點系統的弱點與可疑行為進行，提供獨立與整合的政策設定，允許管理員針對違反政策的系統，採取主動行動、警報、網路隔離、惡意軟體修復等。

偵測來源



EPP單一管理平台

條件比對 跨模組聯動 落實政策 自動執行

7大類自動化回應

個資合規處理

手動搜尋個人資料
隱私活動通知
執行電腦安全評估

修補與弱點處理

執行所有修補
執行特定修補
立即套用修補

通知與通報

發送通知
事件提示
寄送報表

威脅處置

惡意程式掃描
終止程序
刪除/還原檔案

網路阻斷

隔離端點網路連線
(透過 V3 / EDR)
解除端點網路隔離

軟體與資產檢查

檢查軟件安裝
匯入共用資料夾資訊
停用共用資料夾

達成效益

縮短應變時間

減少人工切換與誤操作

落實資安政策

提升端點可視性

強化治理於合規稽核

保留事件處置與鑑識軌跡

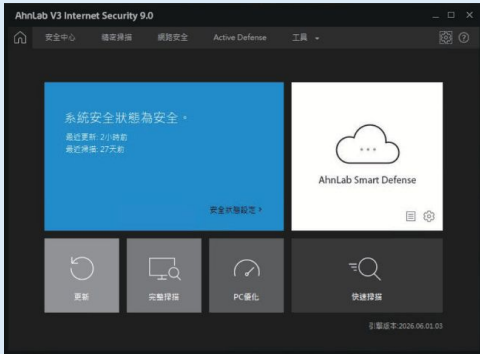
🔍 AhnLab EPP 自動化協同防禦，減少人工追蹤負擔

透過跨 V3、EPM、EDR 的聯動規則，例如防毒掃描未完成時自動提醒使用者並重新啟動掃描，或在偵測到可疑行為時限制外接裝置存取與網路權限。這些原本仰賴人工追蹤與操作的工作，交由系統依規則自動執行即可。



V3 Endpoint Security 端點安全防護

提供全面的個人電腦安全防護，因應各類資安威脅，為企業端點帶來更強而主動的保護，協助建構穩固的使用環境。



快速、強大且全新的端點保護方法



強大的端點保護和惡意軟體防護

- 透過多維分析平台偵測與封鎖惡意軟體
- 針對新的惡意軟體和變種提供主動式防禦



利用SmartScan提供快速精確的掃描

- 以SmartScan為基礎，掃描速度可提升6倍
- 掃描速度更快，並將資源使用量降至最低



使用輕量級引擎

- 採用AhnLab的TS Prime引擎和雲端ASD引擎
- 獨家引擎優化技術，記憶體使用量最小化



簡單強大的防護與高效率的使用者介面

- 可透過主螢幕輕鬆檢查安全狀態
- 輕輕一按，即可掃描或執行系統最佳化功能

V3 威脅防護與勒索軟體應對

多維度惡意軟體分析能力與雲端機器學習強化偵測

雲端檢測分析(ASD)

提供來自雲端威脅分析系統 ASD (AhnLab Smart Defense) 的數十億筆資料，即使未更新簽名檔，仍能支援即時偵測

惡意網址/IP檢測

偵測並阻止來自惡意網址/IP 的惡意軟體下載至系統

Active Defense

- 提供即時分析資訊，例如程式活動
- 提供威脅情報
- 支援自動雲端分析



基於惡意軟體DNA的檢測

- 透過 DNA 掃描偵測變異體
- 預先驗證最初偵測到的檔案

基於信譽的檢測

- 依據信譽封鎖未驗證的程式
- 簽章更新前的主動防禦
- 支援使用者設定信譽條件

行為分析引擎

- 阻擋零時差攻擊
- 可分析超過1000種的惡意威脅行為

EPP Patch Management (EPM)

EPM 軟體更新管理透過集中化管理介面，自動化部署與監控系統更新及安全修補，協助企業維持端點的最新狀態與防護水準。

以端點安全平台簡化軟體更新管理



修補程式實驗室

透過內部修補程式實驗室驗證修補程式的可靠性

整合管理

透過單一管理和基於 AhnLab EPP 的代理程式減輕管理負擔

完整性驗證

透過完整性驗證支援空氣封鎖系統的修補程式更新

支援依資安建議修補清單自動套用重要更新

支援 Microsoft Office 與常用應用程式的自動修補，並可依參考建議修補清單自動挑選與套用高風險更新

網路頻寬設定

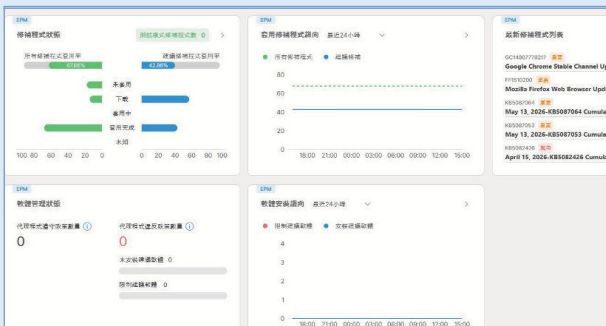
透過以下方式確保作業穩定性及業務連續性，提供修補程式更新的網路頻寬設定

系統強化

透過整合各種以 AhnLab EPP 為基礎的安全解決方案，提供端點系統硬化

EPM 主頁面

EPM 主頁面集中呈現各端點的更新與修補狀態，讓管理者一眼看出未套用更新與風險程度，協助安排處理優先順序。



套用修補程式列表

列表顯示各應用程式的修補明細，包括修補名稱、類型、套用日期與狀態，方便管理者追蹤更新進度並確認端點是否已符合安全要求。

自動化更新部署

自動搜尋並部署作業系統及應用程式的最新安全更新，減少人工操作與遺漏風險，協助企業在不影響日常作業的前提下持續維持端點為最新狀態。

修補程式名稱	KB編號	嚴重程度	修補程式狀態
KB10833	MS03-001	緊急	Unchecked Buffer
KB12262	MS03-003	重要	Flaw in httpd
KB10577	MS03-005	重要	Unchecked Buffer
KB14076	MS03-008	緊急	Flaw in Windows
KB331953	MS03-010	重要	Flaw in RPC End
K3330984	MS03-014	緊急	Cumulative Patch
KB17787	MS03-017	緊急	Flaw in Windows
KB11493	MS03-013	重要	Buffer Overrun in
KB11114	MS03-018	重要	Cumulative Patch
KB19021	MS03-007	緊急	Unchecked Buffer
KB19039	MS03-021	重要	Flaw in Windows
KB23559	MS03-023	緊急	Buffer Overrun in
KB17606	MS03-024	重要	Buffer Overrun in
KB21557	MS03-027	重要	Unchecked Buffer

風險評估與報告

提供修補風險評估與報表功能，能依弱點嚴重度與影響範圍，協助企業先處理高風險更新，並可依風險等級自動制定與套用更新政策，讓管理團隊以更少的人力完成更智慧的修補管理。

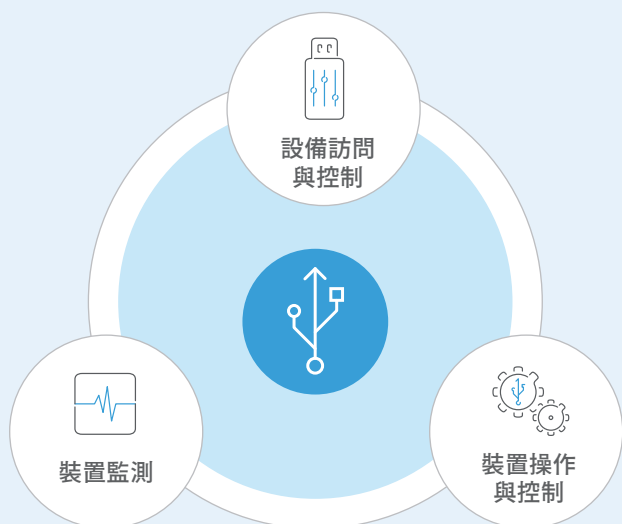
修補程式名稱	修補程式分類	修補程式編號	KB編號	嚴重程度	修補程式狀態
未套用	第三方修補程...	Chrome Enterprise...	GC14807778217	重要	Google Ch
未套用	第三方修補程...	Firefox 151.0.2	FF1510200	重要	Mozilla Fir
未套用	錯誤報告	Chromium Edge 14...	CE1480396783	重要	Microsoft
未套用	第三方修補程...	Adobe Acrobat DC...	AC2600121563	重要	Update av
未套用	第三方修補程...	Adobe Acrobat Re...	AR2600121563	重要	Update av
未套用	錯誤報告	Chromium Edge 14...	CE1480396770	重要	Microsoft
未套用	Microsoft Offi...	Microsoft Office 365	OC3850000	緊急	Microsoft
未套用	Microsoft Offi...	MS-CR202420164	CR202420164	緊急	May 13, 20
未套用	Microsoft Offi...	MS-CS202120670	CS202120670	緊急	May 13, 20
未套用	Microsoft Offi...	Office C2R 2021 R...	OC2021001	緊急	Office C2R



AhnLab EPP Device Control (EDC) 裝置控制

AhnLab EPP Device Control 是建置在新世代端點安全平台上的裝置存取與操作管控解決方案，可細緻管理 USB、外接硬碟等多種裝置，甚至支援到匯流排層級的控制，並提供完整的事件紀錄與統計報告，協助企業防止未授權裝置存取重要資料，無論威脅來自內部或外部。

保護企業資產並掌握裝置使用風險



裝置存取設定

透過裝置類型與匯流排層級的細緻控管，限制未授權 USB、外接硬碟等裝置連接企業端點，並可依部門或使用情境設定允許或封鎖政策。

裝置讀寫控制

針對已允許連線的裝置，可進一步限制讀寫、複製與列印等操作行為，避免敏感資料被大量匯出，同時保留必要的工作使用彈性。

裝置監測與事件報告

自動記錄所有裝置的允許與封鎖事件，並提供統計報告，企業可輸出一段期間的裝置封鎖報告，清楚掌握哪些終端會私接設備而遭封鎖，協助資安稽核與事後調查。

產品穩定性與易用性



產品穩定性

AhnLab 累積多年端點防護經驗，提供超過 15 種裝置控制條件，涵蓋 USB、外接硬碟與行動裝置等設備，並支援匯流排層級的精細控制，穩定套用政策並即時反映裝置使用狀態。



簡易管理選項

透過集中管理介面即可註冊與管理大量裝置例外，並依使用者、部門或時間區段彈性設定允許與封鎖規則，減少逐台調整與溝通成本。



儀表板與報告

儀表板提供清晰的裝置控制狀態總覽，自動記錄所有允許與封鎖事件，並可輸出統計報告，例如某段期間哪些終端會私接設備而遭封鎖，協助資安稽核與事後調查。



AhnLab EPP Privacy Management (EPrM)

AhnLab EPP Privacy Management 是一套專為個人資料保護設計的解決方案，能在端點上盤點並管理含有個人資料的檔案與系統，偵測異常存取或外洩風險行為，並透過集中管理平台提供一貫的保護政策。藉由更完善的個資管理機制，協助企業降低個資法規遵循壓力，並強化對外的信任形象。

從掌握到防護，全面提升個人資料保護

EPP Privacy Management



以生命週期為基礎的
個人資料管理與應變

從個人資料產生的那一刻起即進行檢測與管理。偵測並防止個人資料經由各種管道外洩。

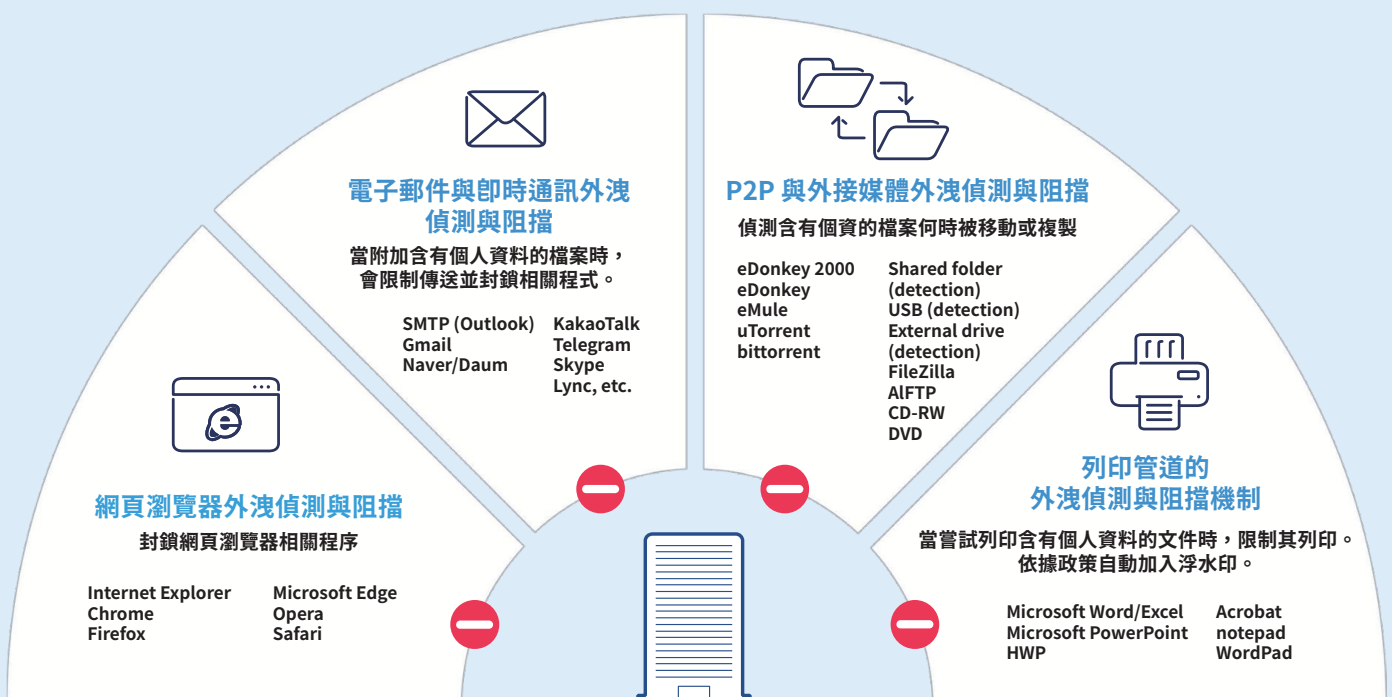


符合《個人資料保護法》的
技術性保護措施

以 AhnLab EPP 平台為基礎，建置整合式的端點個資管理機制，對個人資料、惡意程式與可疑操作提供一致的管控與稽核功能。透過單一代理程式與集中管理主控台，企業得以更方便地落實技術性保護措施與管理義務。

產品穩定性與易用性

AhnLab EPP Privacy Management 會偵測並阻檔含有個人資產的檔案，防止它們在端點透過各種管道外洩。針對個人資料外洩的行為，會於各種管道上即時偵測並應對，全面強化企業環境。





AhnLab EDR 優異的端點偵測與回應

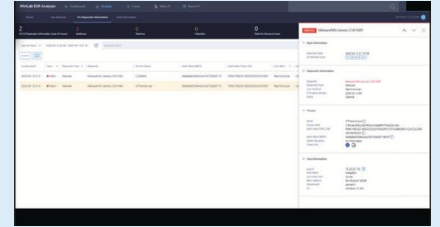
AhnLab EDR 已通過 MITRE ATT&CK Evaluations 驗證其偵測與回應主要威脅技術的能力。2025年的第七輪測試中，AhnLab EDR,EPP,XDR實現了 100% 的防護率。

第七回合



AhnLab
100% Protections
Robust Defense Powered by
Precise Cross-Domain Detections

- 1 模仿技術 Turla
- 2 AhnLab EPP 防止模擬攻擊程序
- 3 公佈結果
- 4 檢討教訓與學習 從結果到產品改進的持續發展流程



<AhnLab EDR 檢測介面截圖>



成功攔截測試中所有的惡意活動，保證了環境和系統安全。已證明其對先進威脅近乎完美的防護能力

以機器學習強化的進階威脅偵測與分析

AhnLab EDR 透過機器學習技術，結合雲端累積的大量威脅與行為資料訓練模型，強化對未知與進階攻擊的惡意程式偵測與行為分析能力。

特色

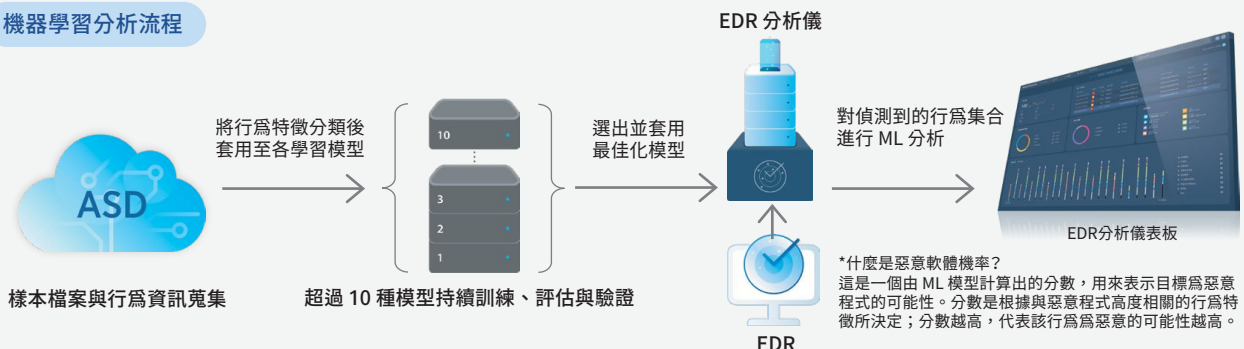
- 針對未知與變種惡意程式的行為分析進行最佳化
- 以行為式分析補強傳統靜態偵測的限制，降低誤判
- 持續分析端點異常行為，提升可疑威脅辨識能力
- 經多模型驗證後，自動套用較合適的分析模型

* 行為特徵：指由多種端點行為資訊組成的分析特徵，包含程序、檔案、網路、系統與登錄機碼等活動，以及相關的 URL、IP 與程序關聯資訊。

效益

- 建立一致的可疑事件判斷基準，利於優先排序與例外管理
- 提升威脅可視性，減少人工分析負擔
- 透過相似事件自動分群，加快研判與應變速度

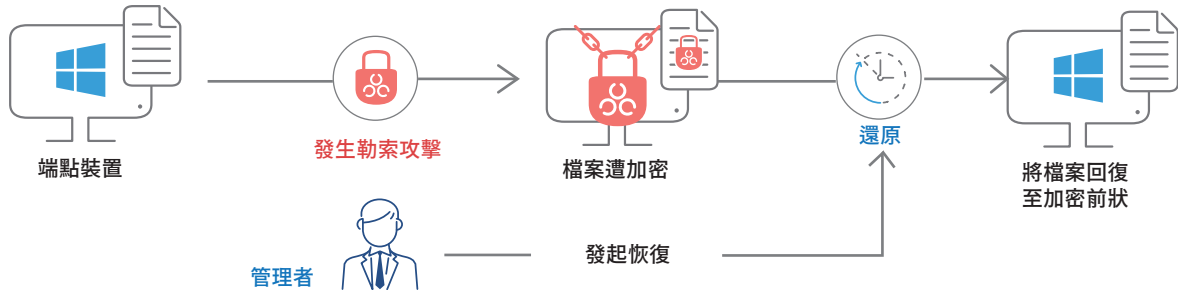
機器學習分析流程



EDR 協助將遭勒索加密的檔案還原至加密前狀態

AhnLab EDR 透過端點快照與回溯機制，在偵測到勒索攻擊後，將遭加密或異常變更的檔案回復到加密前的可信狀態，降低資料損失風險。

還原流程



EDR 的還原功能



將遭勒索加密或異常變更的檔案還原至攻擊前狀態
 依端點或群組設定回復權限與快照建立週期
 執行檔案回復並可初始化端點上的還原快照
 在回復完成或失敗時通知使用者與管理者
 偵測並阻擋停用快照功能、刪除快照等惡意行為

*若直接對 VSS 採取強制性安全措施，可能導致系統不穩定，因此透過監控與阻擋惡意關閉或刪除快照的行為來降低風險

Enable rollback
 If there is no snapshot when using rollback, a snapshot will be created immediately regardless of the cycle.

Cycle hours

Performance issues may occur if the snapshot creation cycle is shorter than 4 hours. Up to two snapshots are created, and the one with the oldest performance time is deleted.

Notify agent when restore point creation succeeds or fails
 Initialize snapshot when EDR agent is deleted

EDR 橫向追查與證據蒐集回應

AhnLab EDR 可由單一可疑端點延伸追查至多台相關裝置，蒐集事件痕跡、系統資訊與調查資料，協助管理者進行更完整的威脅分析與事件回應。

1 偵測與分析可疑行為



2 收集與分析報告和工作



3 收集檔案並執行全面檢查

EDR 分析儀
Ahn鑑識分析

全面檢查和收集



- 搜尋名稱、雜湊值、大小、路徑、建立與修改時間
- 安全地收集為壓縮檔案

Auto AhnReport/Artifacts Collection



- 預設和自訂條件
- 提供專屬檢視器

可收集資訊		
OS/ 系統	系統資訊	防火牆/防火牆規則
	啟動程式資訊	網路存取資訊
	製程資訊	DNS 快取資訊
	任務排程資訊	路由表
HW	服務資訊	NetBIOS 資訊
	註冊資訊	主機檔案資訊
	程式應用程式資訊	ARP 快取資訊
	更新資訊	IP 設定
網頁瀏覽器	裝置、處理器、驅動器、主機板、磁碟、印表機等。	WinSock
	瀏覽歷史、快取資訊等 (IE, Chrome)	視窗事件日誌
安全產品記錄	安全事件日誌	
安全解決方案	V3 檢查資訊	系統事件日誌
		應用程式事件日誌

如對AhnLab 產品想瞭解更多，我們提供產品介紹及免費試用，歡迎來電洽詢(02)2515-1585

AhnLab x 湛揚科技

湛揚科技 T-tech System Corp. | 台灣總代理

湛揚科技成立於2005年，致力於『端點防護、網路安全及資料備份』解決方案，協同合作夥伴為企業提供新世代高性價比的資安產品及專業服務為宗旨。湛揚科技2025正式代理AhnLab，同時也是Acronis™安克諾斯®、WithSecure™唯思安全®台灣總代理，在AI及新型網路技術的快速發展下，湛揚科技將持續專注企業所需有效對抗新威脅的解決方案，並以專業『防毒、備份、雲安全』等新世代資安服務為發展目標，持續為企業及合作夥伴提供優質的解決方案及服務，以『客戶滿意、永續經營』為湛揚科技的使命及價值。

我們的客戶



湛揚科技 AhnLab總代理
www.t-tech.com.tw

台北：(02)2515-1585 技服電話：(02)2515-1599
南區：(07)972-7388 技服信箱：support@t-tech.com.tw