台灣區代理商
湛揚科技

AhnLab MDS

憑藉強大的可視性實現終極威脅響應

針對網路、電子郵件和端點的全面威脅偵測，
透過威脅可見度實現多層次、最佳化的回應

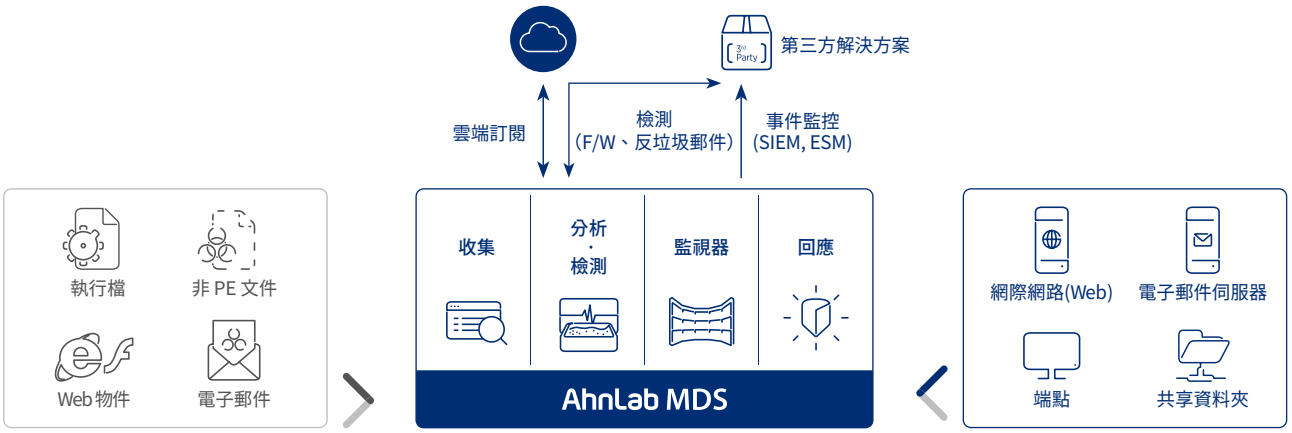
無論行業類型或規模如何，大多數組織都會不斷面臨以新的和未知的惡意軟體、勒索軟體、魚叉式網路釣魚和其他有針對性的攻擊形式出現的高級持續性威脅 (ATP)。
AhnLab MDS（惡意軟體防禦系統）是一種基於沙盒的解決方案，它使用 AhnLab 開發的專有多引擎來精確檢測透過各種媒介滲透到系統中的威脅。它根據威脅可見性提供全面的網路和端點級響應以及有效預防威脅的「收集-檢測/分析-監控-響應」流程。

使用基於多引擎的混合分析來偵測未知威脅或變體
- 基於簽名、信譽和機器學習的靜態偵測
- 基於沙盒的動態行爲分析

收集並分析透過多種來源滲透的威脅
- 網路流量、郵件內容及附件的收集與分析
- 可疑檔案收集及終端異常進程分析

透過整合和互通性對威脅進行多層次回應
- 網路和終端層級的整合回應
- 與現有或第三方安全解決方案的互通

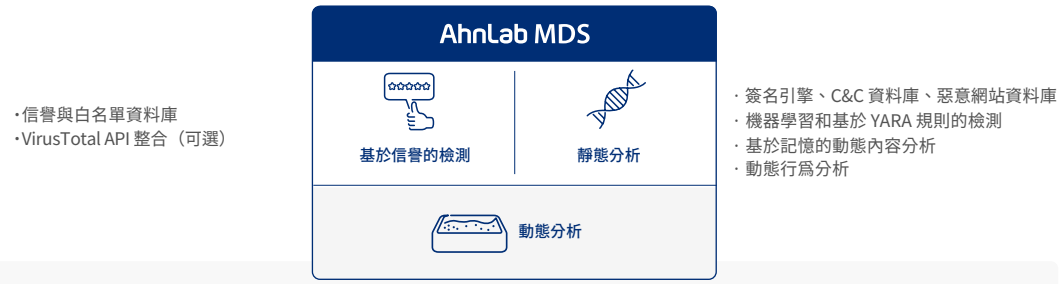
根據威脅可見性爲每個攻擊階段提供最佳化措施
- 攻擊流程圖顯示威脅類型、感染媒介、相關性和偵測狀態
- 針對特定和相關攻擊階段的最佳化回應



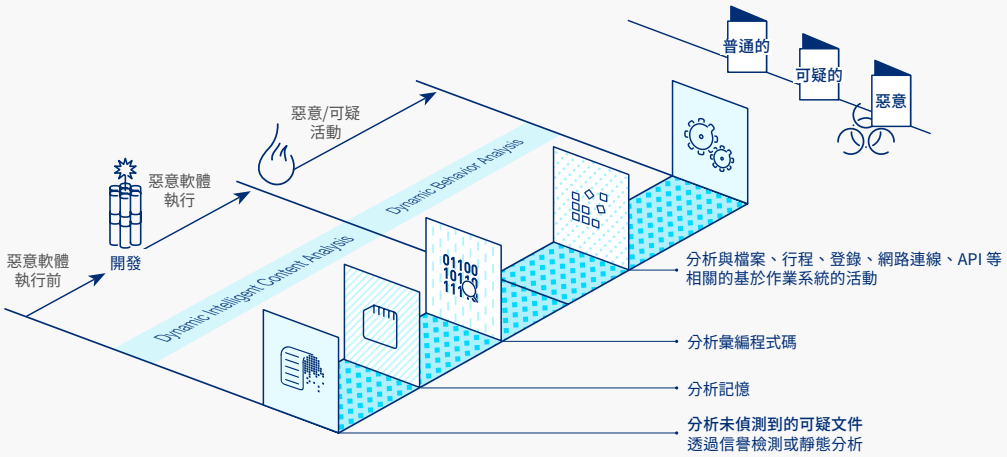
基於多引擎檢測·分析

AhnLab MDS 利用其多引擎功能執行基於簽名的靜態和信譽檢測以及基於沙盒的動態分析，以檢測已知以及新的和變種的威脅。它還使用其專有的記憶體分析來有效地檢測和防止利用，從而遏制試圖繞過沙盒分析的難以捉摸的威脅。

*漏洞利用：利用應用程式錯誤或漏洞來啟動惡意活動的一系列命令

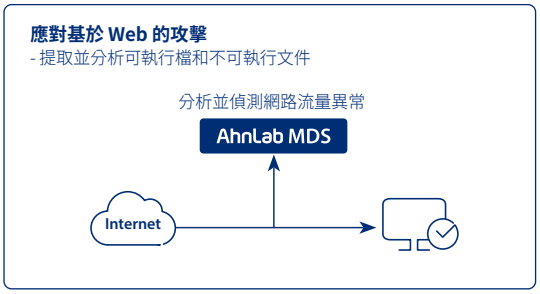


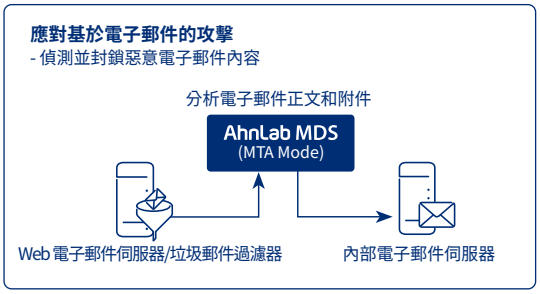
基於沙盒的動態分析流程

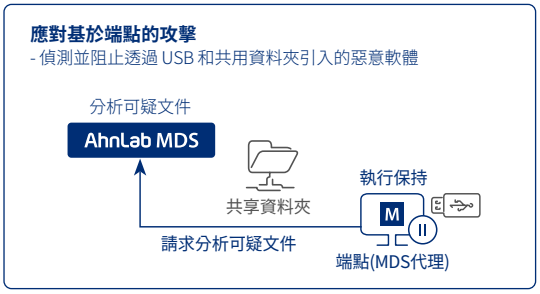


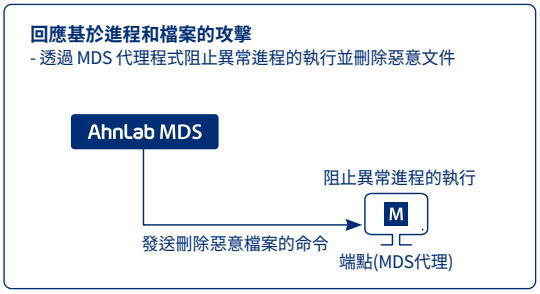
針對多種攻擊的最佳化回應

AhnLab MDS 收集、偵測和分析透過網路、電子郵件和端點等各種媒介滲透的威脅。它還根據威脅類型在網路和端點層級提供有效的回應。 AhnLab MDS 憑藉其輕量級代理，可以在端點暫停執行或收集可疑文件，主動關閉潛在威脅。



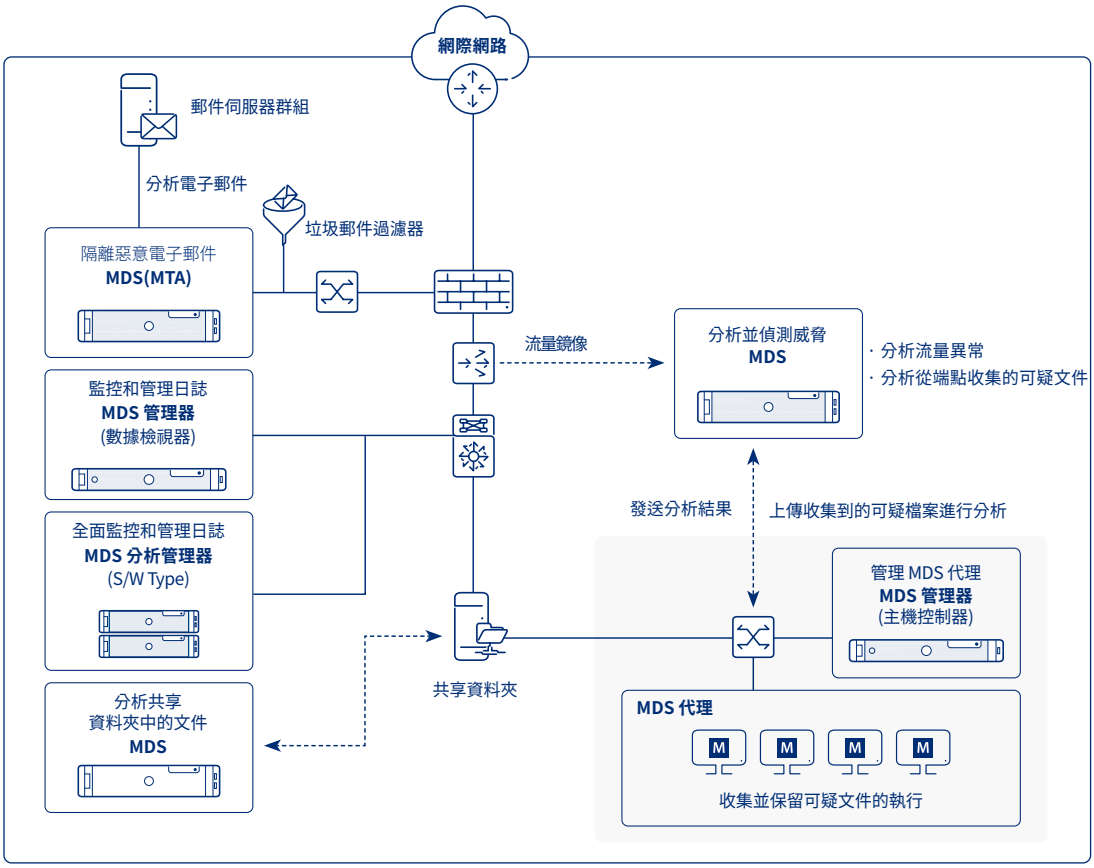






元件和部署

AhnLab MDS 是由用於偵測和分析威脅的 MDS、提供綜合監控和管理的 MDS Manager 和 MDS Analysis Manager（S/W 型）、以及專用於終端威脅回應的代理程式 MDS Agent 組成的完整的先進防護解決方案。



MDS：基於多引擎的威脅偵測與分析

- 檢查和分析各種網際網路服務協定（HTTP、SMTP、SMB/CIFS 和 FTP）
- 偵測並隔離惡意電子郵件和附件（套用 MTA 授權時可用）
- 透過基於沙盒的動態分析和基於簽名和機器學習的靜態檢測來識別新的和未知的惡意軟體
- 採用其獨特的非 PE 惡意軟體分析引擎（MS Office，Hancom Office 等）
- 提供基於 PCAP 的資料包擷取和 PCAP 檔案下載，用於 VM 分析和 C&C 檢測
- 透過 MDS 管理器和雲端來源共享 MDS 設備的行爲分析結果

MDS 管理器：整合監控與管理

資料檢視器：MDS 設備的集中監控與日誌管理

- 在使用者直覺的儀表板上提供威脅狀態和事件訊息
- 提供事件類型、IP 位址以及檔案、進程、登錄和網路上的行爲的詳細日誌
- 整合和管理網路上部署的 MDS 設備偵測到的事件和日誌
- 分發 MDS 設備的行爲分析結果（防止重複分析）
- 互通與管理 YARA 規則
- 以 CEF 和 LEEF 格式轉送系統日誌

主機控制器：整合 MDS 代理管理與回應

- 安裝、修補和設定 MDS 代理程式的群組和原則
- 透過 MDS 代理發送回應命令和通知

MDS 分析管理器：MDS 設備的統一監控與日誌管理（S/W 類型）

- 提供與 MDS 管理器的資料檢視器相同的功能
- 支援 IP 多租用戶，使系統管理員能夠存取和操作多個站點

MDS 代理：對端點中可疑檔案的回應

- 使用機器學習技術從主機系統中提取和收集可疑文件
- 對疑似受感染的主機系統做出回應，包括惡意軟體清除、系統隔離等
- 偵測異常進程並對可疑檔案進行執行暫停

系統需求

AhnLab MDS

	MDS 4000A	MDS 8000A	MDS 10000A	
代理數量	700	2,000	5,000	
流量吞吐量	1Gbps	2Gbps	5Gbps	
HDD	1.2TB x 2ea.	1.2TB x 4ea.	1.2TB x 8ea.	
RAID 配置	RAID 1	RAID 10	RAID 10	
網路介面	1GbE 4 Ports (Copper) 1/10G SFP+ 4 Ports (Optical)	1GbE 4 Ports (Copper) 1/10G SFP+ 4 Ports (Optical)	預設	1GbE 2 Ports (Copper) 1/10G Base-T 2 Ports (Copper) 1/10G SFP+ 4 Ports (Optical)
			可選擇	1GbE 2 Ports (Copper) 1/10G Base-T 4 Ports (Copper) 1/10G SFP+ 6 Ports (Optical)
電源	750W 雙重供電			
波形因數	1U (19”)	1U (19”)	2U (19”)	
規格尺寸(WxDxH)	482 x 721.91 x 42.8mm	482 x 721.91 x 42.8mm	482.4 x 715.5 x 86.8mm	

*注意：效能值依系統配置和網路環境而有所不同
*注意：如果超出代理程式數量，則需要額外的 MDS Manager 設備

AhnLab MDS 管理器

DV（資料檢視器）：MDS 設備的集中監控與日誌管理
HC（主機控制器）：整合 MDS 代理管理與回應

	MDS Manager 5000BR		MDS Manager 10000BR	
代理數量	HC+DV Combined	HC Dedicated	HC+DV Combined	HC Dedicated
	2,000	5,000	5,000	10,000
CPU	1 * 3.30GHZ, 6Core		1 * 3.30GHZ, 6Core	
RAM	32GB		64GB	
HDD	1TB x 2ea., 2TB x 2ea.		2TB x 2ea., 4TB x 2ea.	
RAID 配置	RAID 1		RAID 1	
網路介面	1GbE 2 Ports (Copper)		1GbE 2 Ports (Copper)	
電源	400W Redundant		800W Redundant	
波形因數	1U (19”)		2U (19”)	
規格尺寸(WxDxH)	437 x 503 x 43mm		437 x 647 x 89mm	

*注意：效能值依系統配置和網路環境而有所不同

AhnLab MDS 分析管理器

	MDS 分析管理器
類型	軟體
作業系統支援	CentOS 8 或更高版本
系統需求	CPU: 8Core, 3.0GHz, MEM: 24GB, HDD: 2TB, SSD: 1TB
建議配置	CPU: 16Core, 2.4GHz, MEM: 64GB, HDD: 4TB, SSD: 2TB
多租戶服務	Max. 100 sites supported

AhnLab MDS Agent 的系統需求

	OS Support
客戶端電腦	Windows 7 SP1 (KB4490628, KB4474419) / Windows 8(8.1) / 10 / 11
伺服器	Windows Server 2008 SP2 (KB4493730, KB4474419), Windows Server 2008 R2 SP1 (KB4490628, KB4474419), Windows Server 2012 / 2016 / 2022

*上述作業系統均支援 32 位元和 64 位元

台灣區代理商 湛揚科技
www.t-tech.com.tw
北區：02-2515-1585 南區：07-972-7388

AhnLab