CloudCoffer

DATA SHEET

MatrixShield

未知威脅偵測系統

應用威脅已不容忽視

在現代數位化的世界中，隨著企業仰賴 Web & API 構築各種類型的雲服務，安全性變得越來越重要。攻擊者也變得更加狡猾和複雜。傳統的 Web 應用防火牆 (WAF) 在阻擋已知威脅方面效果顯著，但對於未知威脅和零時差攻擊，仍有許多挑戰需要面對。這時候，MatrixShield 這個革命性的產品應運而生，為企業提供了一個強大且智能的解決方案，來應對這些現代化的安全威脅。

MatrixShield 是一款先進的網頁應用層威脅偵測系統，利用人工智能 (AI) 技術對封包流量進行深入分析，偵測並分析各種攻擊行為，同時識別並盤點 API 行為。其獨特之處在於，它採用旁接架構，通過從 WAF 已分析並阻擋以之威脅後的流量進行鏡像分析，確保系統的安全性和穩定性。

獵捕潛藏於 OSI Application Layer 未知威脅

AI 驅動的威脅分析

MatrixShield 利用最新的 AI 技術，可以分析超過 400 種維度的攻擊行為。無論是已知卻未被有效阻擋的攻擊模式，還是尚未公諸於世（未知）的零時差攻擊，MatrixShield 都能精確識別並給予詳細報告。這使得 MatrixShield 成為企業防範高階攻擊的利器。

未知威脅辨識

未知威脅不僅於一般認知的尚未被公諸於世的零時差攻擊，在許多情況下，由於程式開發的歷史原因，WAF 會設置一些白名單來允許特定流量。這些白名單可能成為攻擊者利用的漏洞。MatrixShield 能夠檢測並告警這些白名單漏洞，確保安全策略的完整性。

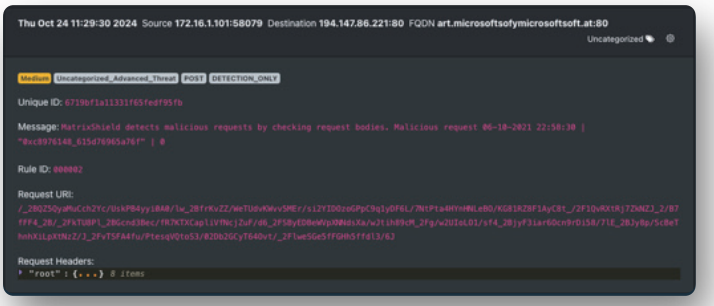
MatrixShield 的 AI 系統能辨識流量中的多種類型威脅，包括尚未被公告於 MITRE CVE 漏洞的零時差攻擊，與應阻擋而為阻擋的已知特徵類型威脅。這使得企業能夠提前防範潛在的安全威脅，減少損失。

全球情資系統

分布在四大公有雲平台上的超過 16 萬台 Honeypot 所構建的全球情資系統，持續收集最新的攻擊情報。這些情資幫助驗證現有威脅偵測模型的有效性，並作為評估 AI 威脅模型始終處於最佳狀態，持續應對最新的網路應用威脅的依據。

導入即偵測

威脅偵測模型在出廠時已完成全面訓練，確保了偵測的準確性和可靠性。這一模型的設計避免了因為 AI 訓練環境和數據內容差異導致的偵測偏誤（如 Data Poisoning），這保證了模型在各種環境下的穩定性和準確性。 。更重要的是，MatrixShield 第一時間即可分析辨識網路流量中的未知威脅，並結合聯合防禦架構即時抵擋攻擊。



AI 辨識尚無威脅特徵特徵的攻擊

CloudCoffer 技術團隊深知攻擊手法不斷演變，為確保 MatrixShield 可持續為客戶偵測各類未知攻擊，透過全球情資系統所蒐集最新的未知威脅，不見斷的驗證 MatrixShield AI 的偵測有效性。

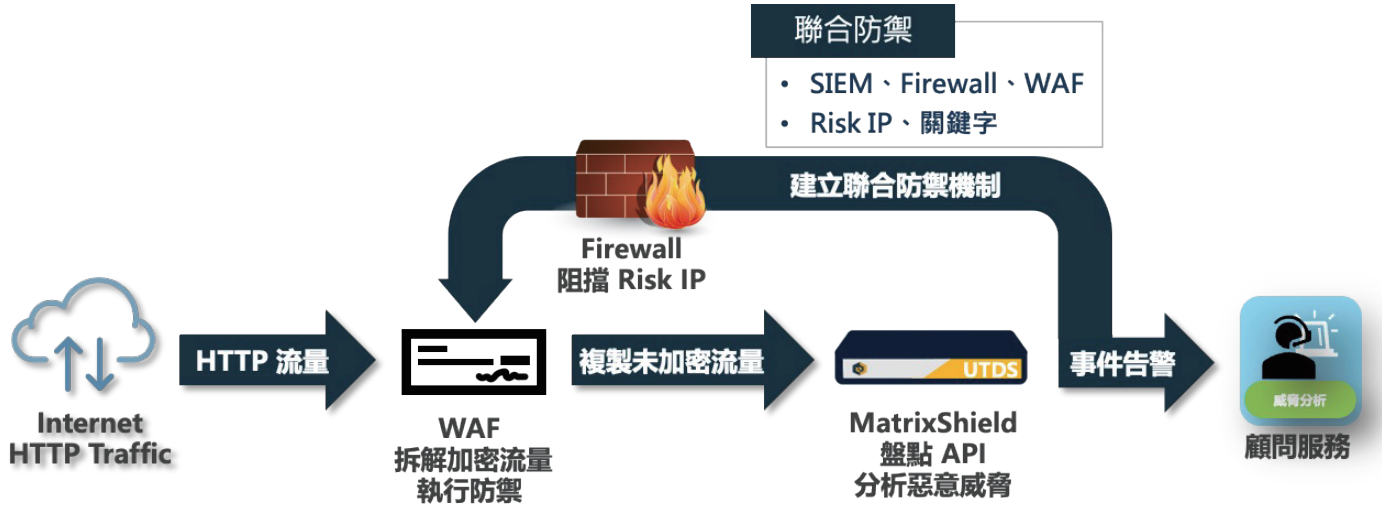
MatrixShield 威脅趨勢統計圖

聯合防禦架構

藉由 WAF 複製已解密的應用服務流量， MatrixShield分析 WAF 已過濾並阻擋後封包內容，獵捕潛藏於其中的未知威脅並驅動聯合防禦措施！

為有效阻擋未知威脅且確保相關應用服務可正常運行，當攻擊發動的第一時間，MatrixShield 透過發送 Syslog 方式告警至 SIEM 或具備 IP 動態黑名單防禦機制產品，阻斷正在發動的攻擊。

MatrixShield 具備攻擊特徵關鍵字自動生成功能，WAF 管理人員可藉由該關鍵字撰寫防禦特徵政策後，完成服務可用性驗證後於正式服務區WAF建立防禦措施，同時兼顧服務可用性與強化防禦的雙重目標。

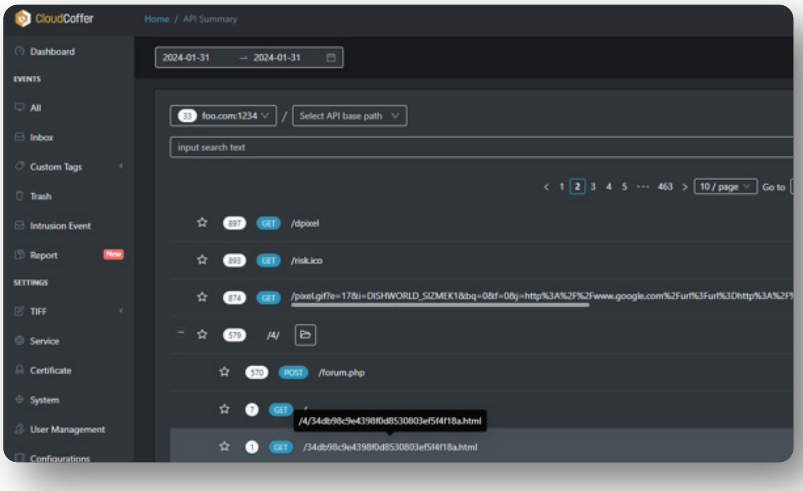


MatrixShield 聯合防禦架構

基於流量即時盤點 API

MatrixShield 提供強大的 API 盤點功能，根據流量自動盤點並生成詳細的 API 使用報告，有效提升了 API 管理的透明度， 幫助企業識別和優化 API 安全策略，防範如影子 API 等潛在的威脅。此功能包括：

- API 詳細資訊：記錄每個 API 的名稱、連線次數、連線方式（如 GET、POST、PUT、DELETE），以及所遭受的攻擊次數。
- 可視化報告：生成直觀的可視化報告，展示 API 的使用情況和安全狀況，幫助企業更好地管理和保護其 API 資源。



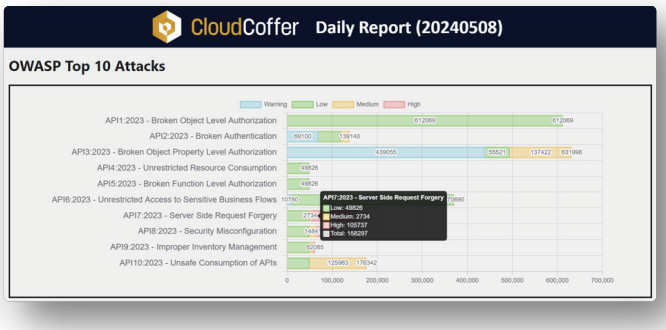
API 可視化偵測與盤點

基於 OWASP API Top10 2023 的威脅分

MatrixShield 具備針對 OWASP API Top10 2023 的威脅分類功能，對偵測到的 API 威脅進行自動分類和分析，具體包括：

- 威脅分類：根據 OWASP API Top10 2023 的分類標準，對所有偵測到的 API 威脅進行自動分類，識別出對應之攻擊類型，並基於 FIRST CVSS3.0 威脅積分機制，建立威脅等級分類。
- 攻擊封包分析：深入分析攻擊封包的內容，自動生成可提升 WAF 防禦能力的關鍵字，進一步提高安全防護水平。
- 自動化聯防：與 SIEM 或防火牆整合，建立自動化的 IP 惡意清單，實現主動聯合防禦，及時阻斷惡意流量。
- 威脅分類報告：MatrixShield 還能生成符合 OWASP API Top10 2023 標準的報告，這些報告可供主管機關或資安稽核單位查核評估，使企業在合規和安全審查中更具優勢。

基於 OWASP API Top10 2023 ＋ CVSS3.0 威脅分類



基於 OWASP API Top10 威脅統計報告

服務不中斷佈署架構

MatrixShield 採用旁接架構，通過鏡像流量進行分析。具體工作流程如下：

- 流量鏡像：來自 WAF 的流量在經過初步分析和阻擋後，被鏡像到 MatrixShield 進行進一步分析。
- AI 分析：MatrixShield 的 AI 系統對鏡像流量進行深度學習和行為分析，識別各種攻擊行為。
- 報告生成：針對識別出的攻擊行為，MatrixShield 生成詳細的分析報告，提供給安全團隊進行進一步處理。

	功能	說明
MatrixShield 未知威脅偵測系統	API 盤點	• API 主機盤點：根據流量數據識別所有 API 主機，並記錄主機名稱與對應的通訊埠號。 • API 詳細資訊：記錄每個 API 的名稱、連線次數、連線方式（如 GET、POST、PUT、DELETE），以及所遭受的攻擊次數。

	API 威脅偵測	• 提供 OWASP API Top10 2023 威脅分類功能，攻擊事件自動分群分類，點擊 Top10 分類即可觀察相關威脅事件紀錄。
		• 提供 FIRST CVSS3.0 威脅積分分級標準，提供 Warming、Low、Medium、High 四種威脅等級分類。
		• API 單一威脅紀錄提供以下資訊：
		  • 日期時間
		  • 來源 IP Address
		  • 目的地 IP Address
		  • 目的地 FQDN （Options)
		  • CVSS 分級
		  • CloudCoffer 威脅分類名稱
		  • Method
		  • Message
		  • Request URI
		  • 攻擊封包原始資料
		• 提供經由惡意攻擊使用的可疑惡意檔案下載，以供資安管理者進行分析，並結合端點防護系統盤點環境內是否出現相同資安威脅。
		• 提供自動生成單一攻擊關鍵字功能，以利 WAF 撰寫 REGEX 進行聯合防禦。
		• 提供攻擊事件驗證功能，可由客戶指向特定的測試環境，重複生成（Replay）單一威脅流量，作為資安防禦驗證評估使用。
		• 提供全 AI 即時威脅分析能力，系統無須聯網更新威脅情資，僅透過 AI 即可分析 API 應用型態與應用服務系統型態等30種威脅分類。

	API 協定與風格支援	• REST • SOAP • GraphQL • gRPC • JSON-RPC • XML-RPC

	報表功能	• 盤點報告：提供 Domain name/ IP Address、Port、Method、Path、Count、Event Count 等統計資訊，以 CSV 格式匯出。
		• OWASP API Top10 2023 威脅事件報表：提供以下分類：
		  • 基於 CVSS 風險等級 Top10 威脅事件統計
		  • 基於 CloudCoffer 威脅分類 Top10 威脅事件統計
		  • 基於攻擊地址來源 Top10 威脅事件統計
		  • 基於X-Forwarded-For 攻擊來源 Top10 威脅事件統計
		  • 基於攻擊目的地 FQDN Top10 威脅事件統計
		  • 基於時間軸威脅事件統計
		  • 基於 OWASP Top10 API 威脅事件統計

	功能	說明
MatrixShield 未知威脅偵測系統	CloudCoffer 威脅分類	• Abused_Protocol • Backdoor_Planted • Bruteforce • Code_Injection • Custom_Rules • DoS • Drupal_Vulnerability • HTTP_Format_Error • HTTP_Disallowed_Policy • JComponent_Vulnerability • Joomla_Vulnerability • Malicious_Agents • Malicious_Domains • Malicious_Incoming_Traffic • Mixed_Generic_Attacks • Outgoing_FilterASP • Outgoing_FilterGen • Outgoing_FilterIIS • Outgoing_FilterInFrame • Outgoing_FilterOther • Outgoing_FilterPHP • Outgoing_FilterEnd • Outgoing_FilterSQL • PHP_Vulnerability • Privilege_Escalation • SQL_Injection • System_Exceptions • Too_Many_Parameters_HTTP_Request • Uncategorized_Advanced_Threat • Warning_Event • WHMCS_Vulnerability
	事件紀錄轉送	• 支援 TCP & UDP 格式之 Syslog 事件紀錄轉拋功能
	網路流量處理效能	• 最高可達 10Gbps (含) 以上處理效能 • 處理效能依據訂閱授權級距
	系統管理功能	• 具備 TLS V1.3 之 SSL 圖形化加密網頁管理介面。 • 具備多種帳號分權管理群組，系統管理者可依據不同的管理帳號及群組對象套用特定管理權限。 • 提供管理帳號登入管理稽核事件記錄、查詢及匯出功能 • 具備管理設定檔備份及還原等管理功能

	型號	說明
MatrixShield 產品型號	MarixShield-Platforrm	• CloudCoffer MaitrxShield 未知威脅偵測系統管理平台一年軟體授權。內含 100Mbps 流量處理授權。
	API-Module-ADD	• 擴增模組: CloudCoffer MatrixShield API 未知威脅偵測模組一年期使用授權，具備 API 盤點與威脅偵測能力，並產製符合 OWASP API Top10 分類報表。
	MarixShield-AD01	• CloudCoffer MatrixShield 未知威脅偵測系統一年期 100Mbps 頻寬增購授權。
	MarixShield-AD10	• CloudCoffer MatrixShield 未知威脅偵測系統一年期 1Gbps 頻寬增購授權。
	說明	
硬體規格需求	系統運行硬體需求：實體機	
	CPU：X86 32核含以上	
	RAM：64GB 含以上	
	SSD：2TB 含以上	
	實際硬體需求規格數量會因擴充模組增加而提高。	