BLUE COAT®

強化公司商務

BLUE COAT 資安分析鑑識平臺

發現、瞭解進階威脅，並對威脅迅速反應

現在的進階惡意程式和零時差攻擊能躲過傳統資安技術的偵測，因此公司企業逐漸接受了自己的網路有時會遭到入侵的現實。也正因此，目前的趨勢正朝向更現代化的策略邁進——希望找出全面性的辦法，能夠提供使用者所需的即時分析能力與智慧，以發現、瞭解進階威脅及針對性的攻擊，做出反應，並保護網路。Blue Coat 資安分析鑑識平臺結合了資安可見度、資安分析鑑識力以及即時的智慧能力，可立即偵測意外事件並有效反應，從而弭平資安上的漏洞。簡而言之，資安分析鑑識平臺可提供進階威脅保護解決方案，讓使用者不用再因每個新出現的資安威脅擔驚受怕——從而能展望業務的嶄新可能。

適應不斷演變的威脅局勢

資安攻擊的數量、種類和來源全都不斷攀升，根據 Kaspersky Lab 的報告，每天會出現 200,000 個以上新的惡意軟體樣本。進階零時差威脅、新世代惡意軟體，以及來自外部甚至內部員工的針對式攻擊，在規模大小上都在不斷上升。

用傳統的封鎖策略應對進階攻擊，成效不彰。隨著資安局勢不斷演變，公司企業與 IT 資安團隊需要可順應趨勢及客製化的解決方案，以克服目前簽章型工具的漏洞，並對網路一切進出提供 100% 的可見度 — 即使面對快速成長的龐大網路流量，也不能失守。為了有效率地處理資安框架不斷擴大的空缺，公司組織還需要簡單、靈活、成本效益高的資安解決方案。

資安分析鑑識平臺是 Blue Coat 進階威脅保護解決方案套件的一環，能弭平資安漏洞，並且抵禦進階威脅，擺平防護中所遭遇的主要難題，特色包括：

- 輕鬆配置簡單靈活的解決方案，能與當前的資安生態系統、程序以及工作流程搭配合作。
- 能夠運用最完善的即時威脅智慧資源，在供擊的前、中、後都能提供完整活動記錄。

92%
的入侵是由外部人員發起

84%
的攻擊發動只在數秒鐘、數分鐘、數小時內就能破壞網路

78%
的攻擊耗時數週、數月或數年才被發現

Verizon Business，2013

- 可隨著企業組織的成長、集中化資安管理的需求、對網路效能增加的需求而擴充。

立即獲得清晰的智慧

資安分析鑑識平臺能夠清楚精準地為資安專家解答遭侵入後的重大資安問題，包括： 攻擊來源？ 攻擊方法？ 攻擊時間？ 哪些地方遭到存取？ 這款獲獎肯定的平臺可以配置在您挑選的硬體上，作為預先組態的設備，或當作虛擬設備來使用，記錄和分類網路流量（從 Layer 2 到 Layer 7）每個封包，同時將資料編列索引並儲存，以便在遭遇資安事件時，提供豐富的威脅智慧和侵入後的鑑識分析。

採用這款平臺能提供可據以行動的證據，實現即時的情境分析、持續監視、進階惡意軟體偵測、資安事件回應與解決、資料丟失監視與分析、IT 管理、 風險控管與法規遵循，以及資安保證。

BLUE COAT®

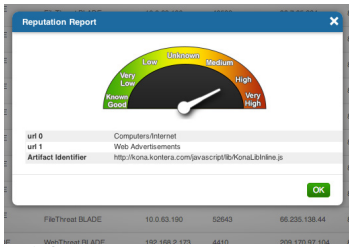
強化公司商務

重要功能與效益

資安分析鑑識平臺是唯一如此靈活、高成本效益且不需依賴硬體的解決方案，同時還能與多款聲名卓越的威脅智慧資源及新世代沙盒技術整合，以達到全面的進階威脅防護。本解決方案可提供：

應用程式分類 — 資安分析鑑識平臺能夠找出任何想躲進您網路的應用程式的真實身份。全面的深度封包檢測（DPI），可分類 1,800 個以上的應用程式，與數以千計的描述型 metadata 詳細資料。這個功能不僅能有效率地辨識應用程式，還可說明網路工作階段的資訊，包括應用程式、使用者身份、行動企圖、內容類型、檔案名稱等等。

即時威脅智慧 — 平臺直接與 Blue Coat ThreatBLADES 整合，能真正發揮重大資安功能。運用 Blue Coat 全球情報網路以及 7500 萬多名使用者的「網路效應」，ThreatBLADES 可針對 Web、電子郵件和檔案型的威脅，提供即時且確實可用的智慧。資安分析鑑識的即時檔案擷取功能還會自動擷取並檢查檔案，立刻自動識別出已知的威脅，避免已知威脅不必要地爆發，進而優化惡意軟體沙盒技術。



即時威脅分析

Layer 2 到 Layer 7 的資安分析鑑識 — 資安分析鑑識平臺可提供多元的海量數據資料分析能力，以全面且確切的分析結果，加強對資安事件的反應。重要功能包括完整的工作階段重建、即時信譽查詢、即時通訊（IM）、電子郵件與影像重建、Root Cause Explorer，且會提供完整的人為產物（artifact），而非僅是封包。

考量情境的資安 — 本平臺採用最優質的網路資安技術，直接利用警報或記錄進行樞紐分析，並取得警報期間及前後的充分負載詳情。開放的 Web 服務 REST API 能帶給所有資安工具完整的情境，並讓使用者能運用 Dell SonicWALL™、 FireEye™、HP ArcSight™、McAfee®、Palo Alto Networks™、Sourcefire®、 Splunk®等資安應用的頂尖技術。

完整的資安可見度 — 透過資安分析鑑識平臺，使用者可獲得數千個應用程式、數十件檔案傳輸、所有流量和封包的分析見解，包括與 Blue Coat SSL 可視性裝置緊密整合而獲得的加密流量。

Root Cause Explorer — Root Cause Explorer 能夠簡化對事件的反應。本工具可利用擷取出的網路物件，重建可疑的 Web 會話、電子郵件以及聊天對話的時間軸。Root Cause Exploer 能自動建立這類事件的時間軸，協助分析師迅速識別出感染或破壞的來源，並能大幅縮短解決問題所需的時間。

靈活部署 — 資安分析鑑識平臺提供多種部署方案選擇，能大幅改善總體擁有成本（TCO），並盡可能將資本支出（CapEx）降至最低，靈活程度非其他解決方案可比擬。本平臺可輕鬆部署在工業標準硬體上，可作為預先組態的設備，或作為全面性的資安虛擬設備，規模小至分公司辦公室，大至企業級的資料中心。

可見化。分析。糾正。

資安分析鑑識平臺提供業界最完善的進階威脅防護解決方案，創造 100% 的網路流量可見度、切實可用的資安威脅智慧，以及靈活、高成本效益的方法，根據需求擴展企業資安。

立刻聯絡當地的 Blue Coat 代表，獲得更多資訊 — 也可為您安排示範解說。讓您的資安防禦和事件應對能力更上一層樓，並為業務培養能力、開創新機。

Blue Coat Systems Inc.
www.bluecoat.com

台灣
電話： 886-2-2528-8718
香港
電話： 852-3476-1000
北京
電話： 86-10-8507-8200
上海
電話： 86-21-5396-6288
廣州
電話： 86-20-2831-7429