Solera 資安分析鑑識設備
Blue Coat 進階威脅保護

資安讓一切
皆有可能

資安分析鑑識設備
快速、可延伸、整體設備，
適合海量數據資料資安分析鑑識

挑戰
企業、服務供應商、政府機構和金融機構在不斷遭受著各種不同型態的網路攻擊。如今的進階威脅、目標式攻擊和自訂惡意軟體在設計上規避傳統的安全基礎結構和基於簽名的工具。對於網路資安缺乏可視性及對於企業各種資安情境的了解，更加劇了發現和遏制各種資安攻擊的複雜性。要有效防禦和保護資訊資產免於遭受進階目標式攻擊，各企業及組織需要海量數據資料所提供的充分可視性。

另外，各企業組織還發現，他們難以部署有效的安全解決方案來實現充分的安全可視性，並提供充分效能及延伸能力，進而符合作業網域內網路流量數量不斷增加的要求。有效的資安分析鑑識解決方案必須能夠：

- 提供即時威脅情報、海量數據資料資安分析鑑識和充分的安全可視性，以延伸到任何規模的企業組織及分支機構，包括從數據中心到遠端辦公室
- 提供高效能和優化的儲存能力，以符合不斷增長的網路流量需求
- 整合現有的安全基礎結構，以充分利用安全工具投資和可靠的程序與工作流程

解決方案
Solera 推出的資安分析鑑識設備為企業提供對先進攻擊的資安絕佳解決方案，它可提供充分的網路安全可視性、情境意識和即時的入侵後安全性。它們採用備受好評的 Solera 資安分析鑑識軟體，該軟體可利用威脅情報數據即時擷取、索引、歸類和充實所有網路流量。資料儲存於特定用途設計、取得專利的資料庫和檔案系統中，以進行快速分析、即時擷取和完整重構，為本領域之最佳資安鑑識分析解決方案。

資安分析鑑識設備可部署於網路中的任意位置：網路邊界或核心、10 GbE 骨幹或遠端連結，以提供明確、切實可行的情報，進而實現即時的情境分析、持續監視、進階惡意軟體偵測、事件回應與解決、資料丟失監視與分析、組織政策合規以及安全保證。

Security Analytics
APPLIANCE by SOLERA

解決方案說明
透過與 Solera 資安分析鑑識軟體整合並預先安裝，資安分析鑑識設備是業界提供海量數據資料和進階威脅保護的標準。

主要特點
- 以資安分析鑑識 Central Manager 進行可延伸、輕鬆和分散式管理
- 與全新的 Blue Coat ThreatBLADES 完全整合
- 使用內建資安分析鑑識儀錶板進行獨立作業
- 具備最高 10 Gbps 封包擷取、索引和分類速率的高效能、整合式設備
- 大儲存容量，可適應延長的歷史擷取視窗
- 採用預先安裝和設定之 Solera 資安分析鑑識軟體進行整體部署
- 運營商級設備：高可用性和維護功能

資安分析鑑識設備是唯一經完整整合的解決方案，用於海量數據資料資安分析鑑識和進階威脅保護，可提供：

應用程式分類 – 超過 1,200 個應用程式和數以千計的描述性、metadata 屬性（包括內容類型、檔案名稱等）將被分類，以便於分析和重新叫用。

即時威脅情報 – Blue Coat ThreatBLADES 直接整合 Solera 資安分析鑑識析設備，並充分利用 Blue Coat 全球情報網路，以便對透過網路、檔案或進階惡意軟體傳遞的威脅提供即時、切實可行的情報。

第 2 至 7 層分析 – 資安分析鑑識平臺可提供各種分析工具，例如：完整的工作階段重構、數據可視化、Root Cause Explorer、時間表分析、檔案與物件重構、IP 地理位置以及趨勢分析。

上下文感知的安全 – 設備採用最優質的安全技術，直接利用警報或記錄進行樞紐分析，並取得入侵期間及前後的充分負載詳情和完整來源證據及事件範圍。

Root Cause Explorer – 這個有效的事件回應程式工具使用擷取的網路物件來重構可疑網路工作階段、電郵和聊天會話的時間表。

自訂的儀錶板視圖，以實現快速分析

媒體面板：檢視所有影像檔案和所有關聯中繼資料

瞭解所有流量和威脅的來源

主要優點

- 獲得情境意識並瞭解安全事件的完整上下文
- 利用第 2-7 層網路流量擷取和內建深度封包檢查 (DPI) 查看事件的每個細節
- 透過與 Blue Coat ThreatBLADES 和全球情報網路緊密整合，直接存取最新的威脅情報
- 加快威脅識別、減少事件回應時間並縮短暴露時間範圍
- 在儲存需要增長時，利用獨立或分散式部署選項不斷擴展
- 自信地部署耐用、已取得認證和經徹底測試的設備
- 以輕鬆部署、整合的整體設備快速取得結果

資安分析鑑識設備

	結構係數	擷取速率（峰值）	板載容量	可延伸容量	介面
 資安分析鑑識 2G 設備	1 RU	2 Gbps	6 TB	3 x 20 TB	3 x 1 GbE
 資安分析鑑識 10G 設備	2 RU	10 Gbps	20 TB	6 x 20 TB	7 x 1 GbE 2 x 10 GbE
 資安分析鑑識 Central Manager	1 RU	不適用	3 TB （不供擷取）	不適用	1 x 1 GbE
 資安分析鑑識析儲存模組	2 RU	不適用	20 TB	不適用	2 x SAS6

Security Analytics SOFTWARE by SOLERA

Security Analytics APPLIANCE by SOLERA

Security Analytics VIRTUAL APPLIANCE by SOLERA

關於 SOLERA NETWORKS，BLUE COAT 附屬公司

Solera Networks 作為 Blue Coat 附屬公司，是業界領先的海量數據資料資安分析鑑識的供應商，從而提供進階威脅保護。其備受好評的資安分析鑑識平臺可對抗進階目標式攻擊和惡意軟體，並就最困難的安全問題向安全專家提供簡明扼要的答案。資安分析鑑識平臺受新一代深度封包檢查和索引技術、完整封包擷取、惡意軟體分析以及即時安全情報與分析能力的支援。全球 2000 間企業、雲端服務供應商和政府機構選擇 Solera，以獲得即時情境意識、持續監視、安全事件回應、進階惡意軟體偵測、資料丟失監視與分析、組織政策合規以及安全保證 – 他們以此可以快速智慧地回應進階威脅與攻擊，同時保護重要資訊資產、儘量降低暴露和損失並降低業務責任。

Solera Networks Headquarters
10713 South Jordan Gateway
Suite 100
South Jordan, Utah 84095

www.soleranetworks.com
info@soleranetworks.com
877-5SOLERA 或 877-576-5372
801-545-4100

BLUE COAT | SOLERA NETWORKS
BLUE COAT 附屬公司