BLUE COAT®

強化公司商務

業界最先進的混合型沙盒模擬技術，用於偵測和分析進階與未知惡意軟體

惡意軟體分析裝置

Blue Coat 惡意軟體分析裝置是 Blue Coat 資安與政策實施中心的關鍵組成部分。惡意軟體分析裝置與 Blue Coat 內容分析系統無縫集成，可在封鎖已知惡意軟體與偵測以及分析未知及進階惡意軟體之間，建立起互通橋樑。

裝置可進行自訂，並採用雙重偵測法提供綜合惡意軟體分析與引發功能。該功能允許您對可疑檔案進行分析，並減少零時差威脅和未知惡意軟體帶來的衝擊。

雙重偵測法：深入偵測惡意軟體行為的最佳方式

惡意軟體分析裝置採用了功能強大的雙重偵測法，兼有代碼模擬和虛擬機自我檢查的優勢。與通常依賴於單一偵測法的解決方案相比，採用雙重偵測法能夠在自訂環境的更大範圍內捕捉到更多惡意軟體行為。雙重偵測法包括：

- Sandbox® – 一個用於模擬實際系統的裸機環境，用於偵測在虛擬環境中不引發的惡意軟體。
- IntelliVM – 可複製實際生產環境（包括自訂應用程式）的虛擬機設定檔，用以快速偵測行為異常，並識別反分析與其他進階惡意軟體躲避技術。

模擬系統：引發藏身的惡意軟體

這項獨有的沙盒模擬技術可模仿裸機環境，以偵測藏身的惡意軟體。惡意軟體分析裝置在模擬器中使用惡意軟體引發功能來執行檔案，就像在真實系統中執行一樣 – 只是沒有在目標 CPU 上執行代碼、載入真實記憶體，或與任何其他物理系統組件進行通訊。

模擬器在核心層級上演習惡意軟體的執行，攔截其行為並將其轉換成分步的鑑定情報。這樣，透過沙盒模擬技術，毋需將實際系統置於任何風險之中，即可得到惡意軟體若在真實裝置中執行帶來的威脅之危害分析圖。

自訂虛擬環境，實現更快的異常偵測

惡意軟體分析裝置採用 IntelliVM 技術，並使用虛擬機設定檔來模擬不同類型的自訂環境，讓您可以快速偵測行為異常，從而識別進階惡意軟體藏身技術。惡意軟體分析裝置能夠在一個安全、虛擬儀控環境中監測一系列系統事件的惡意行為跡象。

分析非常規惡意軟體時，您可以自訂 IntelliVM 功能以增加靈活性，並精確模擬生產環境以偵測進階惡意軟體和目標式攻擊。資安分析鑑識器可以分析它們所選的任何版本應用程式的任何類型威脅。它們能夠準確匹配其組織的桌面環境，並針對瞄準特定組織、準備入侵特定應用程式漏洞的惡意軟體收集相關情報。

共用威脅情報：應用已知資訊，加強安全基礎結構

當未知或進階惡意軟體及零時差威脅被引發時，新威脅情報可在區域的整個安全基礎結構上共用，同時也會透過全球情報網路，在 Blue Coat 的 15,000 位客戶和 7500 萬使用者之間共享。這樣，透過將保護擴大至 Blue Coat 的 ProxySG 安全 Web 閘道，將未知威脅變為已知威脅，並在整個安全基礎結構上共用威脅資訊，可以增加防禦的延伸能力和有效性。

惡意軟體分析裝置的優勢所在

- **卓越的分析能力與準確性** – 獨特的雙重偵測法結合沙盒模擬與 IntelliVM 技術，達到無可比擬的惡意軟體與威脅偵測效能。採用最高匹配模式的自動樣本分類與風險評分，並支援現有惡意軟體分析工作流程，允許您根據潛在惡意活動標記偵測到的系統事件。
- **操作簡易，輕鬆示警** – 即時事故報告中包含事件的詳細分析，可為資安分析鑑識器提供實時通知，同時還提供出色的網頁版使用者介面與惡意軟體進行互動，並提供連續點選安裝程式以識別惡意軟體的功能。使用網頁版儀表板可輕鬆搜尋惡意軟體情報、收集資料庫、儲存樣本、報告以及事件。
- **可延伸的結構與效能** – 每台惡意軟體分析裝置每日可處理成千上萬的檔案，高達 55 台虛擬機上的平行樣本，還可支援多個使用 Windows XP 和 Windows 7 作業系統的虛擬機以及無限制的軟體設定。

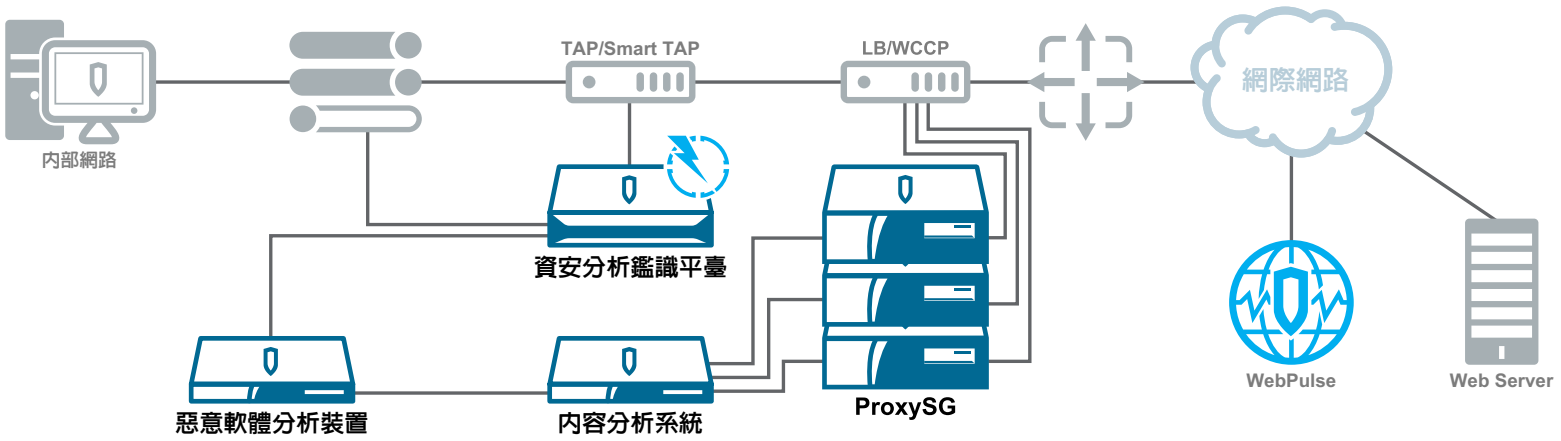
惡意軟體分析裝置系列	MAA S400-10	MAA S500-10
效能		
惡意軟體樣本	每日 12,000 個樣本	每日 50,000 個樣本
系統		
Disk Drives	2 x 500GB	6 x 1TB
RAM	32GB	96GB
內建於機板連接埠	(1) 1000Base-T 銅纜 系統管理連接埠 (1) 1000Base-T 銅纜 BMC 管理連接埠	(1) 1000Base-T 銅纜 系統管理連接埠 (1) 1000Base-T 銅纜 BMC 管理連接埠
供電電源	2	2

物理屬性	MAA S400-10	MAA S500-10
尺寸與重量		
尺寸	572mm x 432.5mm x 42.9mm (22.5in x 17.03in x 1.69in)（僅機殼） 643mm x 485.4mm x 42.9mm (25.3in x 19.11in x 1.69in)（機殼加延伸部份） 1 RU 高度	710mm x 433.3mm x 87.2mm (27.95in x 17.05in x 3.43in)（僅機殼） 812.8mm x 433.4mm x 87.2mm (32in x 17.06in x 3.43in)（機殼加延伸部份） 2 RU 高度
重量（最大）	約 12.8 kg (28 lbs) +/- 5%	約 30kg (66.12 lbs) +/- 5%
操作環境		
電源	雙熱插拔備援電源， AC 電源，100-127V @ 8A， 200-240V @ 4A, 47-63Hz（可選購 DC 電源）	雙熱插拔備援電源， AC 電源 100-240V，50-60Hz，12-5A（可選購 DC 電源）
最大功率	450 瓦特	1100 瓦特
熱功率	一般 1086 BTU/Hr，最大 1381 BTU/Hr	一般 2598.42 BTU/Hr，最大 3751 BTU/Hr
溫度	海平面 5°C 至 40°C（41°F 至 104°F）	
濕度	20% 至 80% 相對濕度，不凝結	
海拔	高達 3048m (10,000ft)	

BLUE COAT®

強化公司商務

適用於所有惡意軟體分析裝置		
規定	**安全性**	**電磁相容性** (EMC)
國際	CB – IEC60950-1，第二版	CISPR22, Class A; CISPR24
美國	NRTL – UL60950-1，第二版	FCC part 15, Class A
加拿大	SCC – CSA-22.2，No.60950-1，第二版	ICES-003, Class A
歐盟 (CE)	CE – EN60950-1，第二版	EN55022, Class A; EN55024; EN61000-3-2; EN61000-3-3
日本	---	VCCI V-3, Class A
墨西哥	NOM-019-SCFI，NRTL 聲明	---
阿根廷	S Mark – IEC 60950-1	---
台灣	BSMI – CNS-14336-1	BSMI – CNS13438, Class A
中國	CCC – GB4943.1	CCC – GB9254; GB17625
澳洲 / 紐西蘭	AS/NZS 60950-1，第二版	AS/ZNS-CISPR22
韓國	---	KC – RRA, Class A
俄羅斯	CU – IEC 60950-1	GOST-R 51318.22, Class A; 51318.24; 51317.3.2; 51317.3.3
環境	危害物質限用指令 2011/65/EU，化學品註冊、評估、許可和限制規例第 1907/2006 號規例	
產品保固	出貨日期起一 (1) 年有限且不可轉讓的硬體保固。 可選購 24/7 軟體支援及硬體支援選項之 BlueTouch 支援合約。	
政府認證	欲獲得更多政府認證資訊，請聯絡 Federal_Certifications@bluecoat.com	
更多資訊	欲詢問特定監管認證問題並獲得支援，請聯絡 regulatoryinfo@bluecoat.com	



Blue Coat 進階威脅保護參考結構。

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