BLUE COAT

安全
強化
企業

解決方案簡介

進階威脅防護

完整生命週期的進階威脅防護方法

每天光是所發現的新惡意程式碼樣本，就超過 10 萬個，而且入侵程式一直在迅速發展並以多樣化方式產生。同時，現今未知的惡意程式碼和零日威脅不斷，甚至可以避開最好的傳統安全防禦。根據 2013 年發佈的 Verizon 資料外洩報告指出，有 84% 的攻擊只需要幾秒鐘、幾分鐘或幾小時就可以危害其目標，而有 78% 的缺口需要幾個星期、幾個月或幾年才會發現。

因此，要朝向一個整合即時防護、動態分析，以及入侵後調查並補救的新方法進行轉移。這個方法會縮小進行中的安全操作與事件發現、遏制和解決之間存在的差距。最終結果是：您的企業可以高枕無憂，轉而將焦點放在各種可能的發展上。

Blue Coat：唯一能夠滿足上述要求的解決方案提供者

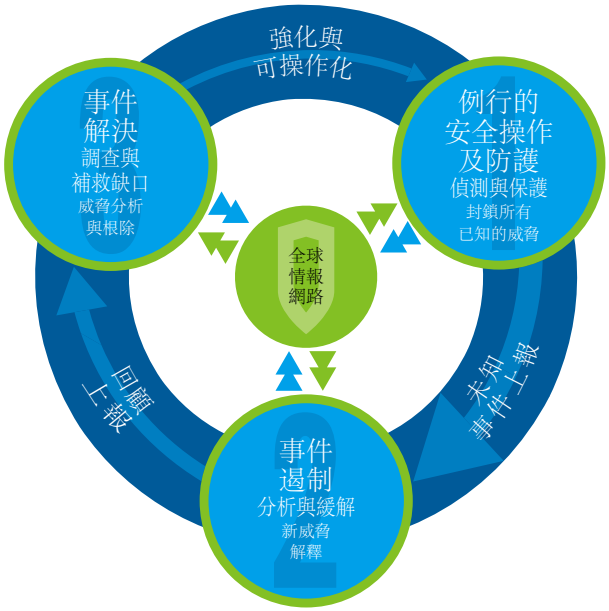
Blue Coat Advanced Threat Protection 解決方案整合來自 Blue Coat Security and Policy Enforcement Center 和 Resolution Center 的技術，透過其 Advanced Threat Protection Lifecycle Defense，爲進階持續性威脅、進階針對性攻擊、進階惡意程式碼、未知的惡意程式碼以及零日威脅，提供一個全面且整合的最新方法。

這種防禦是第一個整合符合您的安全團隊如何使新情報與技術可操作化的業務流程觀點，以強化您的安全基礎設施對抗未來攻擊的防禦方法。Blue Coat Advanced Threat Protection Lifecycle Defense 以三個階段運作：

- **進行中安全操作的偵測與保護**：Blue Coat Secure Web Gateway 以及包含惡意程式碼掃描引擎的 Blue Coat Content Analysis System 可即時防範已知的威脅、惡意來源，以及惡意程式碼交付網路。關於新威脅的內容資訊會在當地共享，並在全球透過 Blue Coat 全球情報網站，以連續反饋迴路方式共享，以擴展威脅知識與防護有效性。
- **事件遏制的分析與緩解**：爲了實現事件遏制，必須使用同時使用 Blue Coat Malware Analysis Appliance 的 Blue Coat Content Analysis System 和 Security Analytics Platform，上報未知的威脅。由於未知或進階的惡意程式碼以及零日威脅的行爲與特性是透過自動化的分析學習，因此該情報會在整個安全基礎設施中共享，從而將防護轉移到閘道，以獲得更具擴展性的防禦。
- **事件解決的調查與補救**：Blue Coat Security Analytics Platform 允許安全事件上報，進行回顧分析，以分析威脅並解決事件。現在已知威脅的情報用於調查與補救整個攻擊範圍，包括網路上已存在之威脅的其他實例。整個攻擊範圍的情報會在當地的安全基礎設施中共享，也會在全球與 Blue Coat 的 15,000 名客戶以及 7,500 萬名使用者共享，使新知識可操作化，並強化安全基礎設施。

BLUE COAT®

安全強化企業



Blue Coat 全球情報網路

階段 1：進行中的操作
- Blue Coat Secure Web Gateway
- Blue Coat Content Analysis System，包含惡意程式碼掃描與白名單分析
- Blue Coat SSL 解密解決方案

階段 2：事件遏制
- Blue Coat Content Analysis System，包含惡意程式碼分析
- Solera (Blue Coat 旗下公司) 的 Security Analytics Platform，包含 Blue Coat ThreatBLADES 和 Malware Analysis Appliance

階段 3：事件解決
- Security Analytics Platform 側錄及鑑識產品系列

圖 1：Blue Coat Advanced Threat Protection 解決方案天衣無縫地結合了當地與全球威脅情報，將未知威脅轉變成已知威脅，提升了安全基礎設施抵禦現今進階威脅的有效性。

共享的威脅情報：強化安全基礎設施

Blue Coat Advanced Threat Protection 解決方案依賴事件生命週期防禦每個階段的當地與全球情報共享，強化安全基礎設施。新的威脅情報不但會在整個安全基礎設施中共享，也會在全球，與 15,000 名 Blue Coat 客戶及其 7,500 萬名使用者共享。

這個強大的網路效應會透過將未知威脅轉變爲未來可以在閘道封鎖的已知威脅，提升防禦的可擴展性與有效性。將新的威脅情報傳遞回閘道的這種方式，可確保對動態威脅與新出現的威脅，進行更快速的預防接種。

最佳解決方案：將您現有的安全投資最佳化

Blue Coat Advanced Threat Protection 解決方案是針對整合到您現有的安全基礎設施而設計，包括 IPS、NGFW、SIEM 以及惡意程式碼沙箱解決方案，讓您部署可以共享資訊的深度防禦方法，以提升防護。

例如，這個解決方案的設計，是充當沙箱解決方案中立且公開的代理人，將未知或可疑的檔案同時傳遞到 Blue Coat Malware Analysis Appliance 和/或其他協力廠商沙箱工具。透過提供檔案在多個系統上進行分析的這個整合能力，您就具備選擇的彈性與自由，建立對抗針對性攻擊與未知威脅的全面性防禦。

BLUE COAT

安全
強化
企業

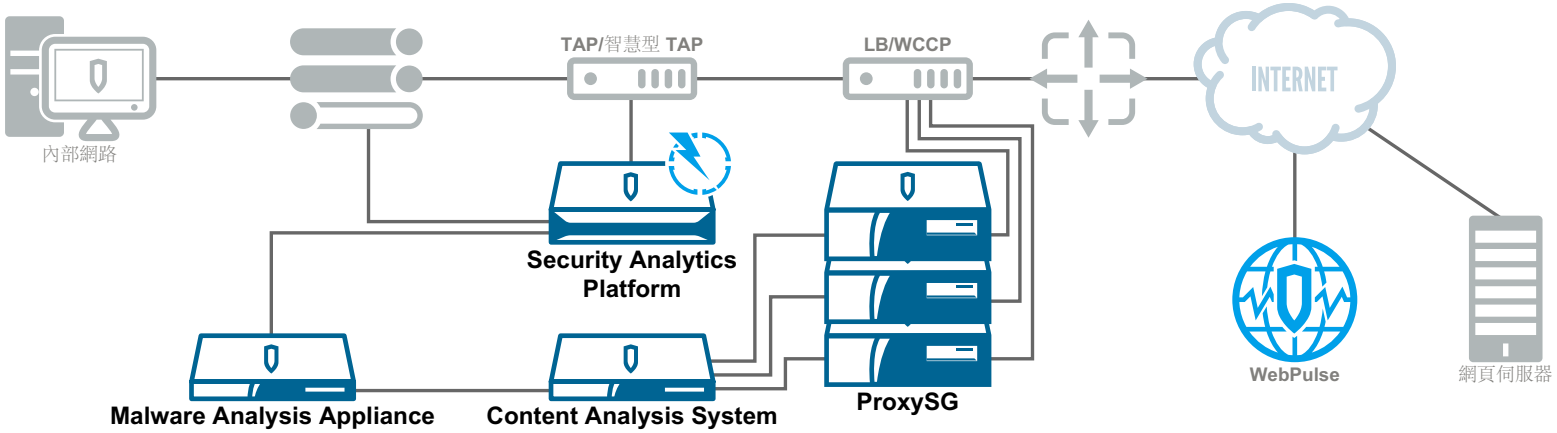


圖 2：Blue Coat Advanced Threat Protection 參考架構

摘要：好處和優勢

Blue Coat 是唯一提供以業務爲導向的資安領先廠商，這個方法會將進行中的操作與威脅偵測、事件遏制以及解決整合在一起。下表摘要說明 Blue Coat Advanced Threat Protection 解決方案的業務優勢。

業務流程導向的防禦	生命週期方法會讓防禦與業務流程保持一致，讓新的威脅情報可操作化，以強化安全基礎設施。
可擴展的有效防禦，以防範零日威脅與未知的惡意程式碼	透過 Advanced Threat Protection Lifecycle Defense，未知的威脅會變成已知的威脅，因此可以將對未來攻擊的防範轉移到閘道來防範。
在全球與當地共享威脅情報	在生命週期防禦的每個階段，新的威脅情報不但會在當地的安全基礎設施中共享，也會在全球，與 15,000 名客戶及其 7,500 萬名使用者共享，以創造網路效應。
最佳化的安全基礎設施投資	Blue Coat Advanced Threat Protection 解決方案會整合到您現有的安全基礎設施中，以便針對進階威脅及惡意程式碼，提供更強大的深度防禦策略。

進一步瞭解

若要獲得 Blue Coat Advanced Threat Protection 解決方案的詳細資料，請立即與您的 Blue Coat 代表安排約會。
如需聯絡資訊，請造訪 www.bluecoat.com。

Blue Coat Systems Inc.
www.bluecoat.com

公司總部
美國加州森尼韋爾市
+1.408.220.2200

歐洲、中東與非洲總部
英國漢普郡
+44.1252.554600

亞太地區總部
新加坡
+65.6826.7000