

第三層：Anti-APT-URL 郵件防護

針對郵件中的釣魚連結 (Phishing URL) 或惡意連結 (Malicious URL)，SEG 會提供：

全新威脅情資比對：透過持續更新的 URL 黑白名單做快速比對與隔離。

未知可疑 URL：做進階檢測與 ToC (Time of Click) 點擊時再做檢測，避免時間差攻擊。

第四層：Anti-APT-File 郵件防護

針對全新未知 (unknown) 的進階惡意程式 (Advanced Malware) 附檔，SEG 會提供：

動態沙箱 (Sandbox) 掃描：將可疑附件打包加密送往雲端做動態沙箱掃描。

全系統模擬 (Full-system emulation) 技術：包括 Windows、Android、Office 文件及 PDF 文件，能夠在短時間內觸發與誘捕潛藏的惡意程式現形。

關聯式分析 (Correlation) 與威脅評分：做威脅等級分析，再回覆 SEG 做隔離或放行。

專業鑑識報告 (Summary Report)：包括惡意威脅評分、惡意檔案名稱、網路活動、處理程序及

寫入機碼 (Registry) 歷程等。

第五層：Anti-BEC 變臉詐騙防護

針對不夾帶惡意附檔或 URL 的 BEC (Business Email Compromise) 商業電子郵件詐騙，提供冒充寄件人 (impostor-based) 的異常郵件檢測與告警機制。

功能特點

個人與群組管理

個人 / 群組黑白名單的設定，以及友善的漏攔回報介面，讓使用者精確檢視郵件。

豐富多元的統計報表

系統可以設定自動報表排程，發送各種統計報表：Top N、圖表、清單等不同型式，同時也可針對個人、群組、IP 作流量統計以及流量監控報告、寄件來源等分析，方便管理者彈性的選擇合適的報表分析。

支援 Word、Excel、HTML 的格式輸出。

使用效益

- 節省尋找重要郵件時間
- 節省刪除垃圾信時間
- 提高員工生產力
- 提升郵件主機效能
- 節省 IT 人員管理時間
- 郵件流量控管
- 個人、群組化彈性管理
- 降低勒索病毒風險
- 降低 APT 滲透風險
- 降低 BEC 匯款詐騙風險

支援郵件系統

- Microsoft Exchange 2016 / 2019 / Microsoft 365 / Exchange Online
- HCL Notes
- Google Workspace
- Sendmail, Qmail, Postfix
- Zimbra

規格表

SEG 型號	50, 100, 250	500, 1000, 2000	5000, 10K, 20k	Service Provider
每日處理郵件數量	5~25 萬封	50~200 萬封	500~2000 萬封	2,000 萬封以上
硬體效能 (可承載人數)	50 ~ 250	500 ~ 2,000	5,000 ~ 20,000	20,000 ~ Unlimited
部署模式	專屬硬體 / 軟體 / 虛擬化 / 雲端服務 / 混合式服務			
Anti-Spam 模組	選購 AG			
Anti-Virus 模組	選購 MAV(McAfee) / BAV(Bitdefender)			
Anti-APT-File 模組	選購 Anti-APT-File			
Anti-APT-URL 模組	選購 Anti-APT-URL			
Anti-BEC 模組	選購 Anti-BEC			

※ 以上產品皆包含一年產品授權及標準保固，可依需求購買 1~N 年保固服務

※ 軟體授權依電子郵件帳號數量計價