

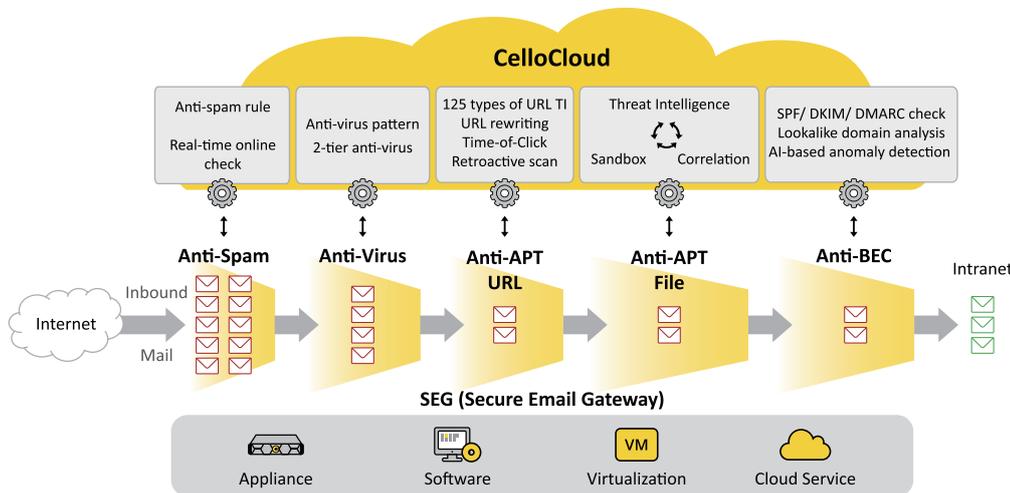


Hassle-free security issues.
Save you time and trouble.

郵件安全閘道器 (SEG)

Cellopoint Secure Email Gateway (SEG) 是部署在 Email Server 前端的整合式電子郵件安全閘道方案，採用獨創 CelloOS™ 技術及業界領先的 CelloCloud™ 雲端安全監控與線上聯防系統，搭配多層掃描機制，能夠有效阻擋日益增多的進階惡意程式 (Advanced Malware)、勒索郵件、垃圾郵件、病毒、釣魚郵件、變臉詐騙郵件、間諜程式、郵件炸彈、跳板攻擊等威脅，幫助您有效做好郵件安全防護管理，提升郵件服務品質。

Security				Archive		DLP	
A	A	U	F	M	G	C	A
G	V	R	L	A	D	S	A
		L	E				U
			C				N
							C
							I
							G
CelloOS							
Email UTM Platform							



郵件的傳輸已成為企業組織最重要的通訊工具，然而大量的垃圾郵件充斥員工信箱，不但造成資源頻寬的浪費，且在垃圾郵件發送的手法不斷更新下，釣魚郵件、病毒郵件更威脅企業的資安防護。SEG 運用五層技術：

第一層：反垃圾郵件 (Anti-Spam)

連線控制 (Connection Control)

在 SMTP 建立連線階段進行檢查，可在郵件威脅進入閘道之前攔阻 50%~80% 的連線，避免佔用網路資源、系統處理效能及儲存設備容量。

DoS (Denial of Service) 防禦 – 防止阻斷服務攻擊 (DoS) 影響您的郵件系統運作。

SRL (Sender Reputation List) 發信來源信譽評等 – 透過全球反垃圾郵件中心 CGAC (Cellopoint Global Anti-Spam Center) 7×24×365 天全時監控世界各地發信來源 IP Address 並給予信譽評分，可即時阻斷不正常發信來源之郵件。

Anti-Relay – 防中繼跳板發送大量垃圾信，避免單位 IP 被 RBL 列為黑名單。

灰名單 (Greylist) – 可辨識正常的寄件端主機，阻擋自動發信程式散播垃圾郵件。

SPF (Sender Policy Framework) – 防止冒用他人郵寄地址發信，驗證寄件人身份。

多層垃圾郵件過濾技術

利用多層的垃圾郵件過濾防護網，搭配 CelloCloud™ 線上雲端資料庫，廣大地蒐集垃圾郵件樣本，並且解讀出垃圾郵件的特徵碼進行比對分析，確保垃圾郵件的防禦率維持 99.9% 以上。

第二層：病毒過濾 (Anti-Virus)

多層式防毒掃描 – 結合先進防毒引擎，提供隨選的病毒掃描與線上更新病毒碼功能，一網打盡各種已知 (known) 的郵件病毒、蠕蟲、間諜程式、木馬程式、勒索及惡意軟體威脅。

解決問題

- 避免重要郵件被垃圾信淹沒
- 避免郵件病毒攻擊
- 減少對外頻寬浪費
- 避免郵件主機遭受攻擊
- 避免 APT 郵件攻擊
- 避免勒索病毒攻擊
- 避免變臉郵件詐騙

特色

- 99.9% 垃圾郵件攔截率
- 99% 病毒郵件攔截率
- 99% APT 郵件附檔攔截率
- 99% APT 郵件 URL 攔截率
- CelloCloud™ 全球監控
- 即時更新郵件威脅情資
- 個人化隔離專區
- AD / LDAP 同步
- Web-based 管理介面
- Syslog 與 CEF log

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。

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 SAV(Sophos) / MAV(McAfee)			
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

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