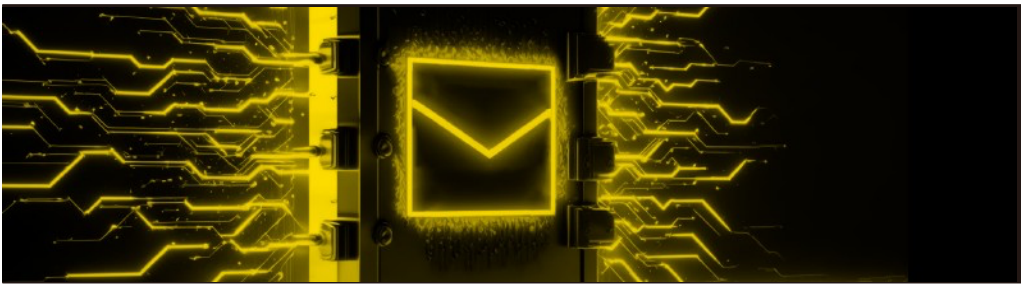
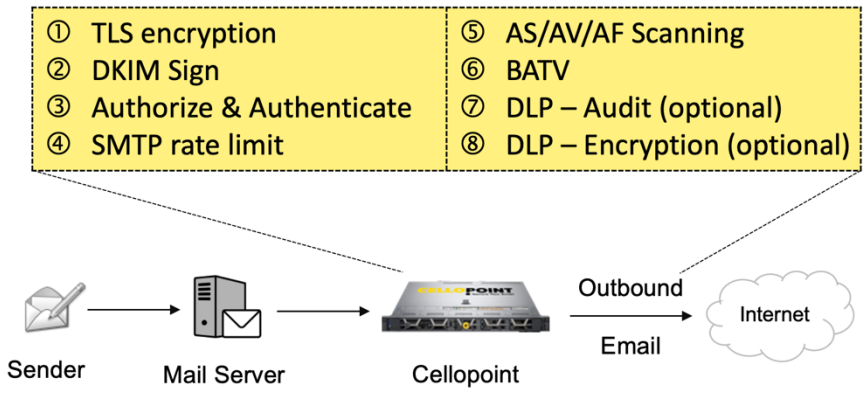


寄外郵件安全與風險管理

COESR (Cellopoint Outbound Email Security and Risk Management) 寄外郵件安全風險管理方案，是專門針對單位組織提供寄外郵件(outbound email)自動化郵件安全傳輸、簽章、認證、監控、掃描、加標籤、稽核及加密政策，以符合供應鏈安全標準、或滿足法規遵循的需求。COESR是基於安全強化與效能最佳化之CelloOS系統，將寄外郵件安全風險管理功能設計為選購式方案，提供彈性擴增或一次購足之需求。

當員工或系統寄外郵件時，系統可自動偵測供應鏈與客戶端之郵件傳輸加密標準，以符合供應鏈安全標準，是否帶有敏感資訊，並針對郵件進行審核、阻擋、轉寄、通知或加密，以幫助組織防止機密資訊外洩、簡化管理及滿足法規遵循的需求。



COESR 郵件安全特色

自動化偵測TLS 安全傳輸

- 支援自動偵測收件端的 TLS (Transport Layer Security)加密版本(v1.0/v1.1/v1.2/v1.3 等版本)，以相同版本進行郵件傳輸。

自動化DKIM驗證機制

- 支援 DKIM 網域金鑰郵件驗證技術(DKIM, DomainKeys Identified Mail)，郵件寄出時可自動插入 DKIM-Signature 及電子簽名資訊，可防止郵件被偽冒或竄改; 同時可以針對多個網域加入不同的 DKIM-Signature。

認證及授權

- 所有寄外郵件皆需進行SMTP AUTH，唯有認證通過才被授權寄外郵件，以確保合法身份能夠寄信。

SMTP rate limit

- 提供多種SMTP rate limit 監控腳本。
- 針對單位時間寄外郵件異常之數量與流量進行監控與處置，包括告警，暫停異常帳號對外寄信。
- 可防止某帳號中毒或被駭，大量寄出病毒或惡意郵件，進而影響到單位信譽。

使用效益

- 寄外TLS安全傳輸
- 寄外自動DKIM驗證
- 支援SPF, DMARC標準
- 寄外認證及授權
- 提升單位寄外郵件信譽
- 節省 IT 人員管理時間
- 寄外郵件流量控管
- 避免外寄病毒信
- 避免外寄釣魚信
- 提升DLP資料外洩保護

CELLOPOINT
Secure Your Email

AS / AV / AF 掃描

系統可做 Anti-Spam、Anti-Virus、Anti-Fishing (URL scanning)、Anti-APT-File (需選購 Sandbox 資源)，避免駭客透過員工郵件帳號寄外郵件，影響商譽。

BATV 機制

- 支援 BATV (Bounce Address Tag Validation)退回地址標籤驗證技術，郵件寄出時自動轉換為 BATV 格式，需選購 Cellopoint 寄內(Inbound)郵件安全模組，可防止退信攻擊。

COESR 風險管理特色

DLP Audit 郵件稽核

條件 + 動作 (Condition + Action)

當預先定義的稽核條件被觸發，COESR 將依據政策提供對應的動作，包含阻擋、通知、轉寄及加密，協助組織監控寄外郵件訊息傳遞，防止不慎或蓄意外洩資料的行為。

DLP Encryption郵件加密

當政策觸發加密動作時，系統會將郵件自動進行加密，包括S/MIME、PDF加密碼、ZIP加密碼、及HTTPs機制，避免郵件在網路上明碼傳輸的風險，保障您的寄外郵件敏感訊息能被安全傳遞，有效施行郵件資料外洩防護。

支援郵件系統

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