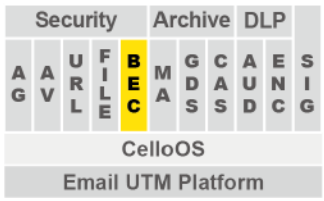
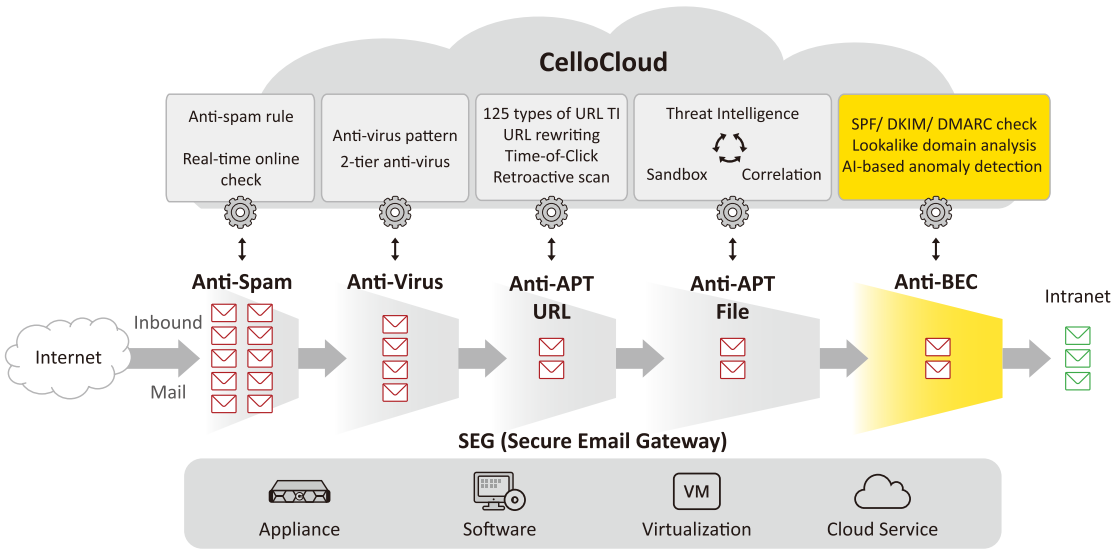
Detect and verify for BEC and fraud email.

電子郵件 BEC 偵測防護

BEC (Business Email Compromise) 商業電子郵件詐騙又稱為變臉詐騙，這是針對公務郵箱入侵、偽冒、潛伏觀察，再利用社交工程手法，誘騙公司或單位財務人員做轉帳匯款，造成巨額損失。這些精心設計的電子郵件，通常在前期透過釣魚 URL 或附件安插後門程式，在取得財務人員的郵箱密碼後，駭客持續觀察郵件往返內容直到出現大額轉帳信息時，偽造對方發送 BEC 變臉詐騙郵件，要求將該筆匯款轉到另外指定銀行帳戶，由於此郵件不帶有 URL 或附件特徵，因此傳統安全閘道器或防火牆幾乎偵測不到。





功能特色

- 顯示名稱偵測
- 寄件帳號偵測
- 寄件網域偵測
- 詐騙情資驗證
- 攔截分析報告
- 智慧偵測與告警

使用效益

- 避免遭受變臉詐騙
- 避免詐騙匯款損失
- 降低營運風險
- 提高郵件安全強度
- 加深資安縱深防禦

郵件的傳輸已成為企業組織最重要的通訊工具，Anti-BEC 進階偵測防禦模組，除了傳統寄件人驗證方式諸如 SPF、DKIM 或 DMARC 之外，此模組採用以下偵測技術，包括：

- 變臉詐騙驗證 (BEC verification) 資料庫，透過智慧型偵測與告警系統，讓使用者驗證真正往來郵件與偽造郵件。

- 顯示名稱 (Display name) 異常偵測，例如：

" 王大明 " <WangDM@cellopoint.com> 竄改為 " 王天明 " <WangDM@cellopoint.com>

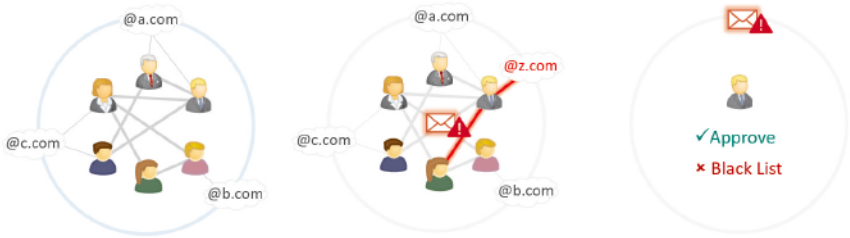
- 寄件帳號異常偵測，例如：

" 王大明 " <WangDM@cellopoint.com> 竄改為 " 王大明 " <Wang_DM@cellopoint.com>

- 寄件網域 (Cousin domain) 混淆偵測，例如：

" 王大明 " <WangDM@cellopoint.com> 竄改為 " 王大明 " <WangDM@cellop0int.com>

CELLOPOINT
Secure Your Email



AI for Modeling **Warning or Blocking** **Identify**

根據使用者行為分析 UBA(User Behavior Analytics) 的特色，Anti-BEC 模組將其應用在詐騙郵件分析上，將每一個郵件帳號收發信的特徵及行為做統計分析，並透過 AI 演算法辨識哪些屬正常，哪些屬異常，並透過人機互動，再進化成更精準的辨識詐騙模型。

AI for Modeling

將個人通聯行為進行塑模，透過人工智慧演算法，找出正常通聯模型與正常寄件人，及異常之陌生寄件人或偽冒寄件人。

Warning or Blocking

系統將可疑郵件暫時隔離，並發出通知信給收件人做告警，再由收件人做確認是否為詐騙郵件。系統可直接將異常的詐騙郵件做隔離。

Identify

可疑郵件經由收件人確認後，可與機器學習系統交互塑模，進而演化更精準之辨識詐騙引擎。