# Smail 郵件安全控管

## 重大資安事件，往往始於一封郵件

外部駭客的釣魚攻擊、勒索軟體的滲透，甚至內部人員有意或無意的資料外洩，都可能透過看似普通的郵件展開。電子郵件不只是日常溝通工具，更是企業營運中最隱蔽卻最高風險的破口。當威脅持續進化、攻擊手法日益精準，傳統的防護措施已不足以因應。

除了攔截與防禦，郵件安全管理同時牽涉資料保存、合規與稽核等關鍵議題。對大型企業而言，需要的不只是防毒與過濾，而是一套兼具智慧防禦、精準策略與組織治理能力的郵件安全控管機制。

外抵威脅內防洩密

智慧防禦快速反應

機敏資料智慧保護

## 大型企業的智慧防禦與分權治理

Smail 郵件安全控管，是一款針對海內外擁有多網域、每日處理百萬封郵件的大型企業需求而設計的防護機制。以 AI 智慧防禦、邏輯決策機制與集團式分權治理，協助企業有效應對零時差攻擊、複雜郵件稽核過濾政策，以及與集團跨組織的郵件管理需求。

### AI 智慧自適應

系統收到漏判或誤判郵件回饋後，AI 引擎可在短時間內自動擷取相關特徵並產出詳細的分析報告，同時啟動系統自我調節機制，阻斷相關威脅。進一步強化企業對零時差、針對型攻擊的防禦韌性。

### 邏輯決策思考力

突破傳統設備的限制，支援多層邏輯的決策思考，滿足複雜的企業稽核與過濾需求。無論是跨國分部特定的郵件流向控制，或縝密的安全稽核，都能透過邏輯決策樹完美達成。

### 集團式分權治理

符合 ISO 安全稽核規定的多層級授權管理，特別適合集團式、需要管控多個網域的大型企業，可針對不同的管理角色，彈性組合定義權限。兼顧總部掌控合規與子公司 / 子網域的管理彈性。

# Smail 郵件安全控管特色功能

### 多層式檔案剖析技術<br>有效抵禦新型態攻擊郵件

有效率分析潛藏附件內文、加密隱蔽、混淆以及無檔案式等混合攻擊手法；差異化行為管理，將威脅和垃圾郵件分區分權管理

### 郵件行為內外控管<br>複雜邏輯一次搞定

針對所有郵件提供邏輯決策樹規則判定，滿足各種管控過濾需求；全方位流向的郵件過濾，防止內部濫發惡意郵件或洩漏重要資料

### 支援多種附件類型<br>依企業需求自訂把關

支援超過50種以上的檔案類型，依企業需求自訂，嚴格把關高風險檔案類型，偽冒副檔名也能察覺

### 獨特的客製報表功能<br>符合需求量身打造

獨特的智慧報表精靈，讓企業能夠依據自身需求彈性設定報表內容，產出符合所需的客製化企業報表

### 專屬的郵件儲存格式<br>節省空間高安全性

經專屬編碼壓縮後的儲存格式，同時保存郵件的 meta 資訊。非明文存取，高安全性；可節省 30%～40% 的空間，效果優於去重複，並真正保留完整資料

### RESTful API化<br>發揮郵件資料價值

全功能皆可以 RESTful API 介面形式，與外部系統整合進行二次開發。讓功能不僅止於過濾與稽核，充份發揮巨量資料的價值

選購功能

多層式檔案剖析

專屬的儲存格式

支援多種檔案類型

彈性設定量身打造

# 成功案例 | 金融租賃企業郵件安全防護

**企業背景**

員工人數約 18,000 人，專注於為高階設備、新能源、公共事業等領域提供金融解決方案

**導入需求**

- 有效攔截日益增長的釣魚郵件和勒索軟體威脅
- 精準防禦「商務郵件詐騙 ( BEC )」，防止合約款項遭篡改或詐取
- 原有的郵件防禦機制老舊，無法應對新型態的社交工程與零時差攻擊
- 符合金融監管法規，需落實機敏資料防護與基本的郵件行為控管

**導入成效**

- 成功阻擋多起針對財務部門的 BEC 變臉詐騙，避免數百萬金額的潛在損失
- 透過多層式檔案剖析技術，有效隔離藏於加密附件中的零時差勒索軟體
- 透過 DLP 落實內外控管，成功稽核並阻擋了多起客戶個資與合約機密的郵件外流

**系統防護規模**

管理網域數
**20** 個

受防護帳號數
**18,000** 個

受防護群組
**280** 個

日均處理郵件量
**70萬** 封/日

Softnext 中華數位科技
TEL:+886-2-25422526 FAX:+886-2-25424838
Email: service@softnext.com.tw
www.softnext.com.tw