



MailSherlock

郵件稽核歸檔系統



MailSherlock

郵件稽核歸檔系統

自 COVID-19 爆發以來，發送電子郵件的數量增加 **55%**。近年國內外的討論中，雖然即時通訊與社交網路，有助於實現工作相關的目標，但是每個人都有一個電子郵件地址，電子郵件具有 **99%** 的市場滲透率，且仍為企業最不可取代的溝通工具。

電子郵件具法律效力

企業或組織對其正確的保存與歸檔，刻不容緩！



Mail-AUDIT

郵件稽核系統可適應個資保護法及資訊安全管理規範之要求，或企業設定的機敏或智慧財產篩選條件，事前防範機敏資料外洩。



Mail-ARCHIVE

遵照資訊生命週期管理(ILM)觀點進行郵件歸檔管理，郵件歸檔系統可保有郵件完整性及不可否認性，符合法規要求之舉證條件。



Anti-VIRUS

為郵件閘道提供首道之安全防護，阻擋電腦病毒與惡意程式危害企業或組織。



Anti-BEC

提供進階郵件防偽辨識技術、多層次的真偽辨識，防堵變臉詐騙來竊取商業機密。

選購



Anti-SPAM

擁有25年自主開發垃圾郵件過濾經驗與技術，能夠更貼近在地文化與時事，有效且快速的過濾垃圾郵件。



Anti-APT

與全球一級實驗室防駭情資中心同步，避免用戶訪問惡意網站，即時防堵最新型網路釣魚及社交工程攻擊。



Cloud Sandbox

提供國際資安大廠(Sophos)強大且高擴展性的仿真隔離環境，動態沙箱對未知或可疑的檔案進行誘發和分析，並提供精細取證的報告。全方位對抗零時差攻擊。

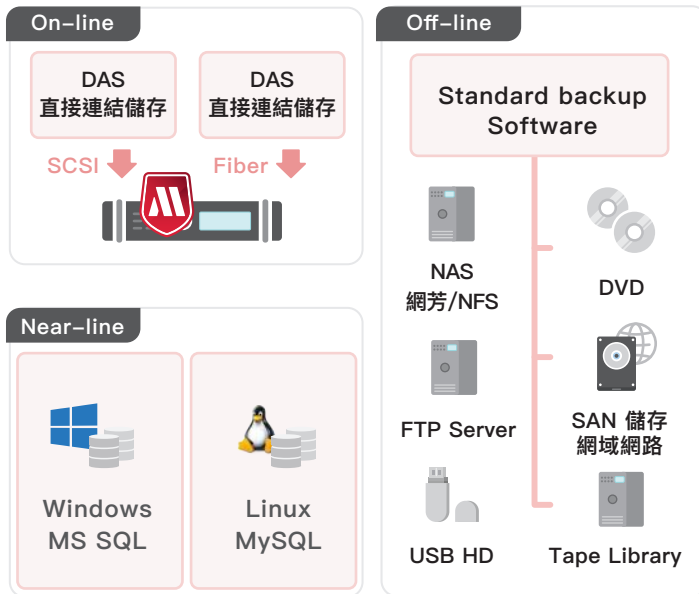
知名案例

- ✦ 2012年三星與蘋果在美國智慧型手機專利訴訟，三星疏於電子郵件保存，未停止電腦系統每隔14天便自動將電子郵件刪除的措施，被蘋果律師發現向法官抗議，並要求懲罰三星。蘋果在一審中獲得勝利。
- ✦ 2016年美國大選，原聲勢大好的希拉蕊因「電郵門案」衝擊下，與總統大位擦身而過。
- ✦ 以電子郵件舉證，在臺灣高等法院98年度上易第1156號民事判決亦有案例可循。

完整郵件防護-防範未然、舉證保存

- ✦ 具備郵件稽核功能，主要防止公司機敏郵件外洩防範於未然，而郵件歸檔則是保有郵件完整性 (Integrity) 及不可否認性 (Non-repudiation)。
- ✦ 符合「行政院資訊安全管理」以及國際電腦稽核協會制定的「內部稽核管理制度」。

郵件歸檔儲存機制



符合個資法保存與舉證要求



郵件完整保存：

- 保存郵件原始MIME檔案(.eml)
- 高達 70-80% 壓縮率的檔案備份機制



郵件調閱舉證：

- 提供郵件資訊多條件查詢機制，例如寄件者/收件者/主旨
- 設定不同等級的調閱權限
- 資料備份加密機制

- ✓ 完整歸檔企業郵件
- ✓ 歸檔郵件全文與多區域檢索
- ✓ 歸檔郵件生命週期管理與保存機制

郵件稽核機制

管理者可自訂義與組織相關之機敏或智財篩選條件來進行郵件寄發前稽核。系統自動保存所有往來信件原檔並快速建立存取機制。支援用戶直接取用，並兼具事前防範與事後取證的功用！



Mail-AUDIT

針對郵件附檔的 Word、Excel、PowerPoint 及 PDF 等文件檔案，進行內容關鍵字過濾及副檔名偽裝偵測，並可對壓縮檔中的文件檔進行過濾，預防機密資料外洩。

Mail-ARCHIVE

提供建立保存與管理歷史郵件之機制，並強化個資安全防護技術，快速進行相關信件事前防洩、事後舉證及責任釐清。

Anti-SPAM

獨創多層次垃圾郵件防堵機制，讓使用者自行設定個人垃圾郵件判定門檻，有效阻擋垃圾郵件。

Anti-VIRUS

提供郵件傳遞一站式郵件服務，整合 ClamAV / Sophos* / Bitdefender* 防毒引擎，即時程式監控與辨識，自動更新病毒碼資料庫，有效攔截電腦病毒與惡意程式。

Anit-APT

主動偵測來往郵件的內文或附件是否遭到 APT 威脅，並可透過系統提供即時隔離、移除或拒收郵件等動作。

選購

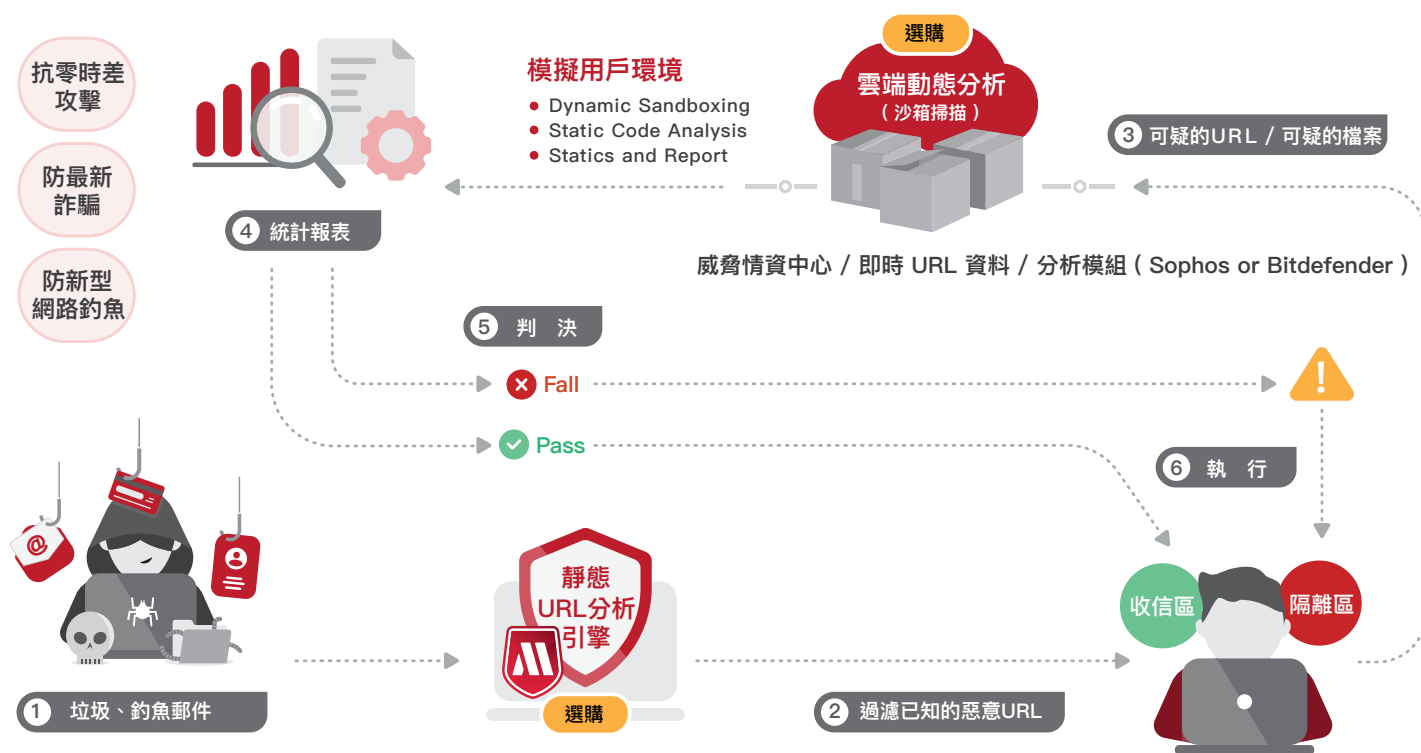
選購

選購

APT 進階攻擊防禦

隨著網路罪犯技術的增長以及駭客跨組織的聯手合作，讓新型惡意軟體日趨複雜且難以捉摸。零時差惡意攻擊不但比過往更加盛行，更針對已知的安全技術和防護進行規避。

- 01 與全球 Tier 1 資安實驗室情資中心同步（實驗室每天分析超過 15 萬筆未知之URL，累計 URL 資料庫超過 20 億筆）。
- 02 阻擋零時差（ZeroDay）惡意軟體攻擊，防堵新型網路釣魚及詐騙，有效地降低針對性攻擊。
- 03 雲端沙箱（Cloud Sandbox）提供擬真安全隔離環境，進行惡意程式分析。
- 04 雲端沙箱（Cloud Sandbox）依據行為模式分析，利用型態辨識偵測多階段攻擊組態及偽裝威脅，阻絕目標性攻擊。
- 05 雲端沙箱（Cloud Sandbox）採精細化取證方式，提供風險評等和攻擊修復所需的細項資訊。



| 產品 | Mail-AUDIT | Mail-ARCHIVE | Anti-SPAM | Anti-VIRUS | Anti-BEC | Anti-APT | Cloud Sandbox |
|--------------|------------|--------------|-----------|------------|----------|--------------|---------------|
| MailSherlock | YES | YES | OPTION | OPTION | OPTION | OPTION (訂閱制) | OPTION (訂閱制) |

標準功能

| 功能項目 | 功能描述 |
|---------|-----------------------------------------------------------------------------------------------------------|
| 管理 | 提供 Web-Based 管理介面相關設定，包括：操作記錄、公司資訊、存取控制、認證設定、存取紀錄、MailSherlock Update。 |
| 網路組態 | 提供網路相關設定，包括：網路介面設定、路由與閘道器、DNS 組態、主機表以及掃描控制。 |
| 郵件伺服器管理 | 提供郵件伺服器相關設定，包括：郵件路由設定、本地端郵件網域、郵件轉寄權限設定、信件佇列查詢、信件佇列設定、進階參數設定、簽名檔設定。 |
| 人員管理 | 提供人員資料與部門資料等管理功能，包括：LDAP 同步設定、UNIX 帳號同步、部門管理、部門階層管理、員工名單管理、Archive 名單管理、管理員帳號管理、MailSherlock 群組管理、帳號認證設定。 |
| 信件查詢 | 提供各類信件資訊查詢，包括：信件查詢、隔離區管理、收信記錄查詢、Sendmail 紀錄查詢、信件還原記錄、備份信件管理、垃圾信提報管理。 |
| 郵件稽核 | 可依部門或特定群組(黑名單)分別設定郵件安全政策，進行郵件控管，管理功能包括：稽核區、規則管理、規則類別、稽核通知。 |
| 統計報表 | 提供各類常用報表，包括：伺服器信件總覽、正常信件統計，正常信件排行榜、連線數統計、放行信件統計、DoS 連線次數統計、報表寄送排程。 |
| 資料庫管理 | 提供資料庫管理功能，包括：資料庫設定、MySQL 帳號管理、資料庫總覽、資料庫檢測、備份檔案管理、郵件備份排成、郵件備份回存、郵件保存期限、Near-line DB 設定、遠端備份設定、資料庫管理警訊。 |
| 系統管理 | 提供作業系統與硬體相關資訊與設定，包括：硬體資訊、硬碟使用狀況、處理程序管理、系統設定檔備份、系統時間、開機與關機、訊息通報。 |
| 日誌格式 | 依據系統所產生事件的 CEF Log，可以更加方便安全地將 Log 匯出至第三方的 SIEM / Log Management 進行整合及自動正規化分析。 |

產品功能 選購區

Anti-APT

- APT 掃描引擎
- APT 機器學習機制
- URL 解析：網路釣魚攻擊、防詐欺連結
- 回溯偵測防禦
- 區域聯防(需搭配 HGiga C&Cm@il 郵件協同系統*)

Anti-SPAM

- 黑/白/灰名單/暫時性黑名單檢查
- RBL 檢查機制
- DNS 記錄檢查
- 寄件者/收件者名單檢查
- 退信攻擊防禦技術
- SpamCheck 過濾引擎
- SpamCheck 自動學習技術
- 自訂過濾關鍵字
- 垃圾信處理機制：標籤/隔離/刪除
- 個人隔離確認：隔離通知信及放行確認區

Anti-BEC

- 檢查 SPF / DKIM / DomainKeys / DMARC
- 檢查假冒本地端寄件者
- 郵件內文寄件者偽照辨識
- 寄件者資訊重複存在偽照辨識
- 寄件者資訊偽照辨識
- 檢查郵件回覆資訊偽照辨識
- 相似網域寄件者偽照辨識
- 不曾來往的網域偽造辨識

Anti-VIRUS

- 防毒引擎 (搭配國際大廠 Sophos* / Bitdefender*)
- 病毒碼更新
- 防毒防制設定：隔離/刪除

Cloud Sandbox

- 雲端沙箱模擬誘發引爆及分析

備註：「*」代表需額外搭配採購項目。



PowerStation 智慧型網路閘道系統

全面進化 SSL VPN、TLS 1.2/1.3 連線相容性、L4 / L7負載平衡服務、整合雙因子資安檢核機制、APT 縱深防禦監控機制、DNS Tunneling Detection 分析、權限管控等七大功能，為企業網路閘道做有效分流與承載。



C&Cm@il 郵件協同系統

高效能、高穩定與高擴充性的郵件系統，全新 RHEL 8 / Rocky Linux 8 作業系統、支援響應式網頁(RWD)設計、整合 MFA 多因子資安檢核機制，讓企業專業形象與競爭力隨著電子郵件的累積而逐日成長。



SpamSherlock 郵件安全防禦系統

超過25年自主開發垃圾郵件過濾經驗與技術，整合 Anti-VIRUS、Anti-SPAM、Anti-BEC等功能，提供進階郵件防偽辨識技術、即時防堵最新型網路釣魚及社交工程攻擊。支援APT進階威脅防禦及雲端沙箱 (Cloud Sandbox) 技術，郵件防禦有保障！



MailSherlock 郵件稽核歸檔系統

強化 Mail-AUDIT、Mail-ARCHIVE 郵件稽核機制，適應個資保護法及資安規範要求，事前防範企業機敏資料外洩；同時保有郵件完整性，符合法規要求之舉證條件。



OAKclouds 企業協同作業入口網

將企業日常管理中的電子郵件、行事曆、通訊錄、公佈欄、會議室管理、問卷調查及電子表單等資訊整合到一個入口平台管理，結合流暢的行動同步，打造高生產力、高安全性的辦公環境。



ADr ID Manager系統帳號管理與整合平台

提供企業內部帳號整合的服務平台，包含：Web-based 的 AD / LDAP 管理、帳號權限控管、SSO 單一登入機制三大功能，集中管理使用者帳密，大幅提升管理者帳管效率！



恒基科技股份有限公司
www.hgiga.com

(恒基科技保有此印刷物內容之異動權利，若有異動恕不另行通知。)

經銷商



SOPHOS

