為提升企業競爭力與工作效率，企業開放各式行動裝置，包含筆電、平板電腦、智慧型手機，包含企業公器與個人私器，意即 BYOD Bring Your Own Device，存取電子郵件系統資料，包含電子郵件、通訊錄、行事曆，此舉無疑增加企業 DLP 營業秘密外洩憂慮。

全球駭客 APT 進階滲透攻擊獲利最高為 BEC 商業郵件詐騙，占比 50% 以上，其攻擊分兩個階段，滲透階段與詐騙階段，滲透階段絕大多數標的為竊取電子郵件資料，以獲得精準個資與情資。

導入 ArmorX Mail MDM 行動裝置控管系統，可對外隔絕企業既有脆弱的電子郵件系統，同時達成企業 DLP 營業秘密外洩防禦與 BEC 商業詐騙滲透防禦的雙重目標。

建置外部存取電子郵件系統

導入 ArmorX Mail MDM 行動裝置控管系統，做法為建置外部電子郵件系統，與既有電子郵件系統一樣，與既有 LDAP/AD 整合，設定允許外部存取的帳號或群組，以及設定帳號允許存取國別與服務，例如 ArmorX Mail APP 或 ArmorX Web Mail。ArmorX Mail MDM 行動裝置控管系統藉由 IMAP(S) 自既有電子郵件系統同步電子郵件，並提供外部使用者 ArmorX Mail APP 或 ArmorX Web Mail 寄信服務。

殺手級別滲透攻擊防禦

ArmorX Mail MDM 行動裝置控管系統作為企業外部電子郵件系統，引用 ArmorX 強大的雲端駭客名單流量清洗，大幅降低來自全球駭客的滲透攻擊與猜密碼攻擊。運用全球獨家帳號存取國別控管功能，協助企業正向表列帳號允許存取國別，例如大部分使用者僅限台灣本島存取，若主管有國外出差需求，開放特定國別，此企業最佳蜜網捕捉技術，大幅提升企業自我安全防禦力，搭配選購 ArmorX APT 惡意電子郵件防禦，可同時達成 BEC 商業詐騙滲透防禦與 APT 進階滲透攻擊防禦。

裝置綁定與資料不落地 APP

為解決使用者密碼遭竊與盜用問題，企業導入 2FA 雙因子認證刻不容緩，ArmorX Mail MDM 行動裝置控管系統支援最安全、便利的裝置綁定技術。

為達成 DLP 營業秘密外洩防禦，ArmorX Mail MDM 行動裝置控管系統支援最新資料不落地技術，可強制不啟用離線資料庫模式，遠端伺服器將所有資料，包含電子郵件內容、附件、通訊錄、行事曆，利用網路 HTTPS 加密傳輸方式，即時顯示於手機記憶體，當使用者權限終止或網路連線中斷時，資料立即清除，全面性消弭資料存放於手機端可能產生的各種疑慮。

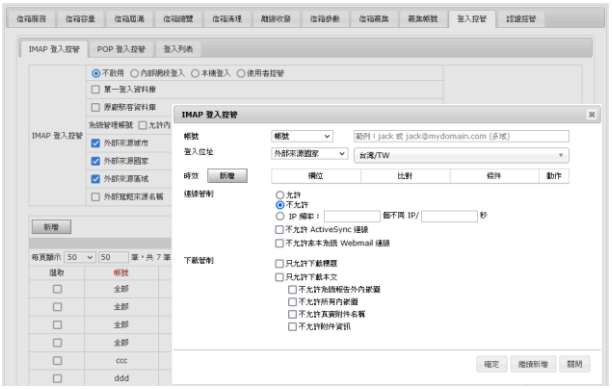
Web Mail 禁止下載郵件與附件

ArmorX Mail MDM 行動裝置控管系統提供 @ArmorX Android APP，可於 Android Play 商店下載與更新。提供 @ArmorX iOS APP，可於 Apple Store 下載與更新。

ArmorX Mail MDM 行動裝置控管系統同時提供安全、好用的 ArmorX Web Mail，支援第三方 OTP 驗證，例如 Google Authenticator，以達成 2FA 雙因子驗證目的，並可設定禁止下載郵件與附件，以達成資料不落地的目的。

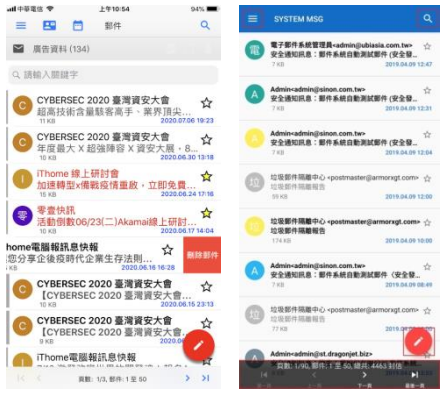
ArmorX 操作介面

帳號國別控管



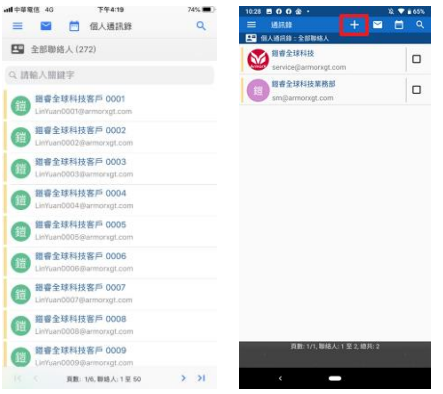
獨家國別讀信日誌

ArmorX Mail APP 電子郵件



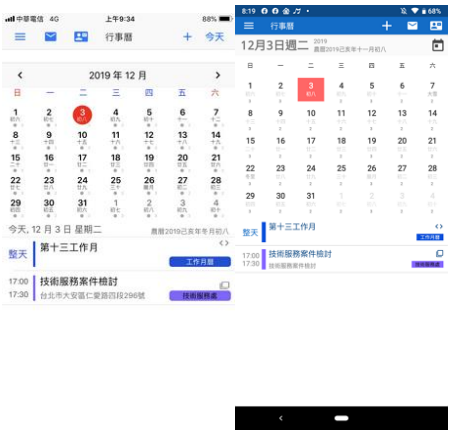
ArmorX Web Mail 電子郵件

ArmorX Mail APP 通訊錄

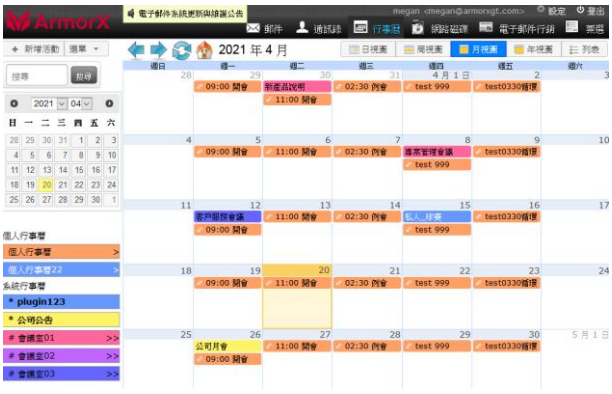


ArmorX Web Mail 通訊錄

ArmorX Mail APP 行事曆



ArmorX Web Mail 行事曆



鎧睿全球科技 Security Defense • Collaboration Platform
極智防護 • 全球最佳 • 資安防禦暨溝通協作

鎧睿全球科技股份有限公司
業務信箱 sales@armorxgt.com
客服信箱 service@armorxgt.com

台北 | 新竹 | 台中 | 高雄 | 海外
總公司 | 30264 新竹縣竹北市自強南路 8 號 21 樓之 3
T 03-621-6700 F 03-621-6799