政府單位案例分享 | 導入產品 Openfind™ Mail2000

一分鐘聊案例

Openfind™
網擎資訊軟體股份有限公司
詳細資訊請查閱
http://www.openfind.com
聯絡電話
(02) 2553-2000 分機 888 業務部

客戶痛點

「國家資通安全發展方案 (110 年至 113 年) 」中明確要求政府單位屬於資通安全責任等級 A 級公務機關最需要優先導入零信任，並預計在三年內分階段逐年導入其 3 大核心機制：身分鑑別、設備鑑別，以及信任推斷。

身為中央政府第一級機關、資通安全法分類的 A 級，無論是自身業務需求，或是配合國家政策，對於資訊安全都是極其重視。該機關是優先需要完成導入身分鑑別的政府單位，而率先整合零信任的 Openfind 產品，立即滿足了其需求。

導入效益

Mail2000 因應零信任 3 大核心精神，配合政府政策提供完整解決方案：

- **身分鑑別**
  1. 鑑別聲明（session-key）驗證可對應鑑別保證等級（AAL）等級 3
  2. FIDO 整合以無密碼（FIDO2）雙因子驗證達成身分鑑別
- **設備鑑別**
  1. 信任裝置完整記錄不同裝置登入狀況
  2. 裝置綁定、保護使用者帳號安全性
- **信任推斷**
  1. 異常登入 IP 警示偵測不合法登入行為（如登入地點或 IP），即時通知
  2. 異常行為分析紀錄與分析帳號登入 Log 或自訂的異常判斷條件
  3. 登入 IP 限制可分析帳號登入 Log 或自訂的異常判斷條件
  4. 權限設定依照需求，可自訂多種保護帳戶和限制權限的設定
  5. MailMDR 情資自動分析事件，在異常事件發生時由專人回報；定時更新最新情資，達到資安聯防效果

Mail2000 整合支援零信任網路，協助公務機關完善法規遵循

身為中央政府第一級機關、資通安全法分類的 A 級，無論是自身業務需求，或是配合國家政策，對於資訊安全都是極其重視。導入網擎資訊 Mail2000 近 10 年來，無論是系統穩定性、功能實用性和服務即時性，一直都頗受長官與同仁好評，特別是在資安方面，Openfind 不僅能夠緊跟時勢，協助機關避免各項威脅，更能與時俱進的滿足國家法規需求。

隨著政府持續走在數位轉型的道路上，「國家資通安全發展方案 (110 年至 113 年) 」中明確要求政府單位屬於資通安全責任等級 A 級公務機關最需要優先導入零信任，並預計在三年內分階段逐年導入其 3 大核心機制：身分鑑別、設備鑑別，以及信任推斷。因此，對於該機關而言，無疑將是優先需要完成導入身分鑑別的政府單位。而率先整合零信任的 Openfind 產品，可說是立即滿足了該機關的需求。

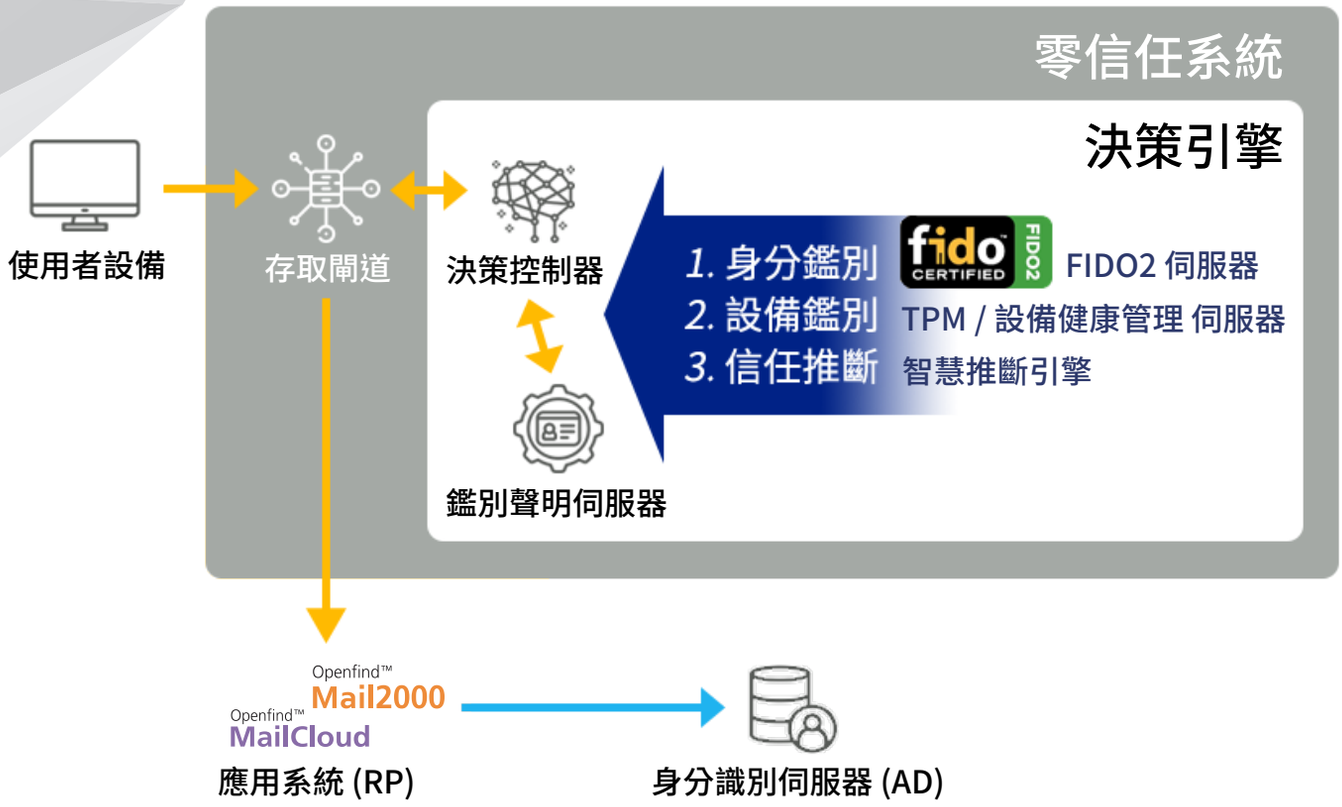
率先整合零信任，高效落實資安政策

對於政府機關乃至一般企業來說，電子郵件時至今日依然是溝通與資訊交流的重要工具，因此 Mail2000 一般來說會是公務單位首先選擇導入零信任的應用系統（PR）。事實上當國家資通安全研究院甫一公布政府零信任架構身分鑑別功能驗證通過廠商名單，Mail2000 就已於系統登入環節整合 FIDO 及生物辨識，並與全景 IDExpert、MOTP 等產品整合，加強登入認證的安全性與順暢度。網擎資訊透過與零信任架構供應商進行整合推廣，打破網路邊界防護的迷思，落實 3A 框架（Authentication 認證、Authorization 授權、Accounting 記錄），讓零信任架構協助政府機關能由裡至外清楚落實資安政策。

建構 Mail2000 安全與便利的零信任架構

該政府機關在現有的 Mail2000 環境下提供使用者透過 Webmail 的方式登入進行收發信，由於現有登入方式僅透過帳號與密碼的驗證登入機制，因此該單位選擇導入全景的零信任 IDExpert 機制並強化使用者登入安全流程。

在具體作法與架構上，該政府機關規劃導入零信任機制之後，所有的 Mail2000 使用者無論從內部或是透過外部連線，當使用者需要存取系統時都需要先經過零信任之網路身分鑑別流程過之後，才能導向允許存取的 Mail2000 郵件系統服務，因此在導入後，使用者將無法透過以往只需輸入帳號密碼驗證方式登入到郵件系統服務。



【零信任網路架構】

配合政府政策提供完整零信任解決方案

Mail2000 V8 版本持續提供符合政府單位所需要的郵件安全環境，其中在資安方面的功能與開發上更貼近零信任機制所提出的 3 大核心精神，相關功能包括：

- **身分鑑別**
  1. 鑑別聲明（session-key）驗證可對應鑑別保證等級（AAL）等級 3
  2. FIDO 整合以無密碼（FIDO2）雙因子驗證達成身分鑑別
- **設備鑑別**
  1. 信任裝置完整記錄不同裝置登入狀況
  2. 裝置綁定、保護使用者帳號安全性
- **信任推斷**
  1. 異常登入 IP 警示偵測不合法登入行為（如登入地點或 IP），即時通知
  2. 異常行為分析紀錄與分析帳號登入 Log 或自訂的異常判斷條件
  3. 登入 IP 限制可分析帳號登入 Log 或自訂的異常判斷條件
  4. 權限設定依照需求，可自訂多種保護帳戶和限制權限的設定
  5. MailMDR 情資自動分析事件，在異常事件發生時由專人回報；定時更新最新情資，達到資安聯防效果

遵循政府資安發展方向，落實零信任精神

零信任（Zero Trust）已逐漸成為政府所關注的資安議題，在面對資安及新興議題上，網擎持續跟進和遵循政府的資安發展方向，並於新版 Mail2000 掌握零信任核心精神，協助政府單位盡早落實零信任相關規劃。Openfind 協助政府核心機關依照零信任的要求與概念提供相對應的功能建置與導入，其中導入的效益包含了提升使用者登入安全與系統安全性兩大方向：

1. 協助政府單位提升使用者登入安全機制

Mail2000 除了搭配裝置紀錄且提供 FIDO 生物辨識認證做為提升多因子認證機制之外，透過 FIDO 提供的 Windows Hello 及 Apple Passkey 等使用者熟悉的認證方式來登入 Mail2000 帳號，無疑是更兼具認證安全及高易用性的登入選擇。

網擎除了可整合全景 IDexpert 的零信任身分鑑別服務之外，也提供 OTP 雙重驗證機制，多樣的身分驗證方式能有效落實使用者登入安全機制。

與此同時，Mail2000 V8 所新增的裝置紀錄功能，可以讓使用者得以隨時查看登入系統的裝置名稱、登入日期、登入地點及 IP，除了讓使用者能更快速了解自己的帳號是否有被盜用之虞，也能對應零信任的設備鑑別精神。

2. 協助政府單位提升郵件系統安全性監控機制

Mail2000 V8 異常登入 IP 警示機制功能可加強系統登入監控機制，因此在資安政策上會將台灣以外的 IP 或登入地點皆列為不合法登入行為，當系統監控到異常登入當下會即時通知管理者，管理者收到異常登入警示可決定要將使用者登出或是變更密碼，所有的異常行為分析都會有完整的 Log 紀錄可以提供給管理者查看。管理者也可以依照不同的資安政策強度決定異常判斷條件，若有異常使用者行為需要進行監控皆可透過自訂異常登入警示方式作為條件通知，以及透過不同的等級直接強制控管使用者的權限與範圍。