Consulting Service – Workshop

自由系統資安解決方案—資料安全管理服務

Data Security and Data Loss Prevention (DLP)

Microsoft

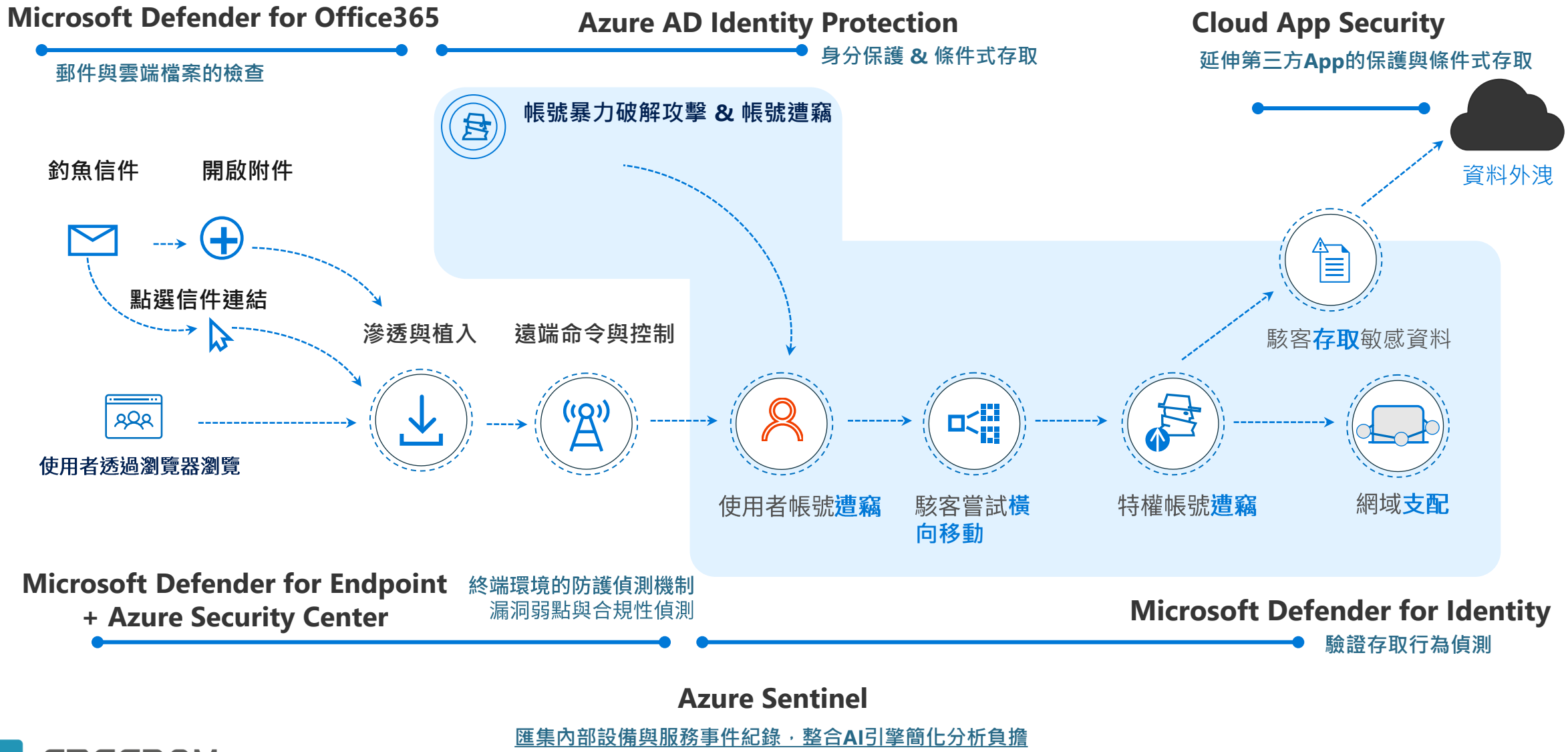
FREEDOM SYSTEMS

自由系統資訊安全服務團隊
Freedom Systems Inc.

Microsoft Partner
Microsoft

Gold Security
Gold Cloud Platform
Gold Cloud Productivity
Gold Windows and Devices
Gold Small and Midmarket Cloud Solutions

智慧化身分保護運行情境流程



自由系統如何建構安全的資訊環境

資料 Data
保障資料本身受到完善的保護與掌控

裝置 Device
保障資料與身分運行在高安全性環境

身分 Identity
保障員工身分僅由本人持有與使用

網路 Network
保障網路傳輸都是合規流量

FREEDOM SYSTEMS

為你的資訊防護旅程做好準備

分類

依照組織法務與商務需求，
訂定對應的分類結構

存取控管

透過原則制定，防堵資料外洩
與遏止惡意資料操作行為

保護

套用企業級資料加密，
建構資料守護城池

偵測

建立多層次警示通報機制，
掌握資料整體狀態與流向

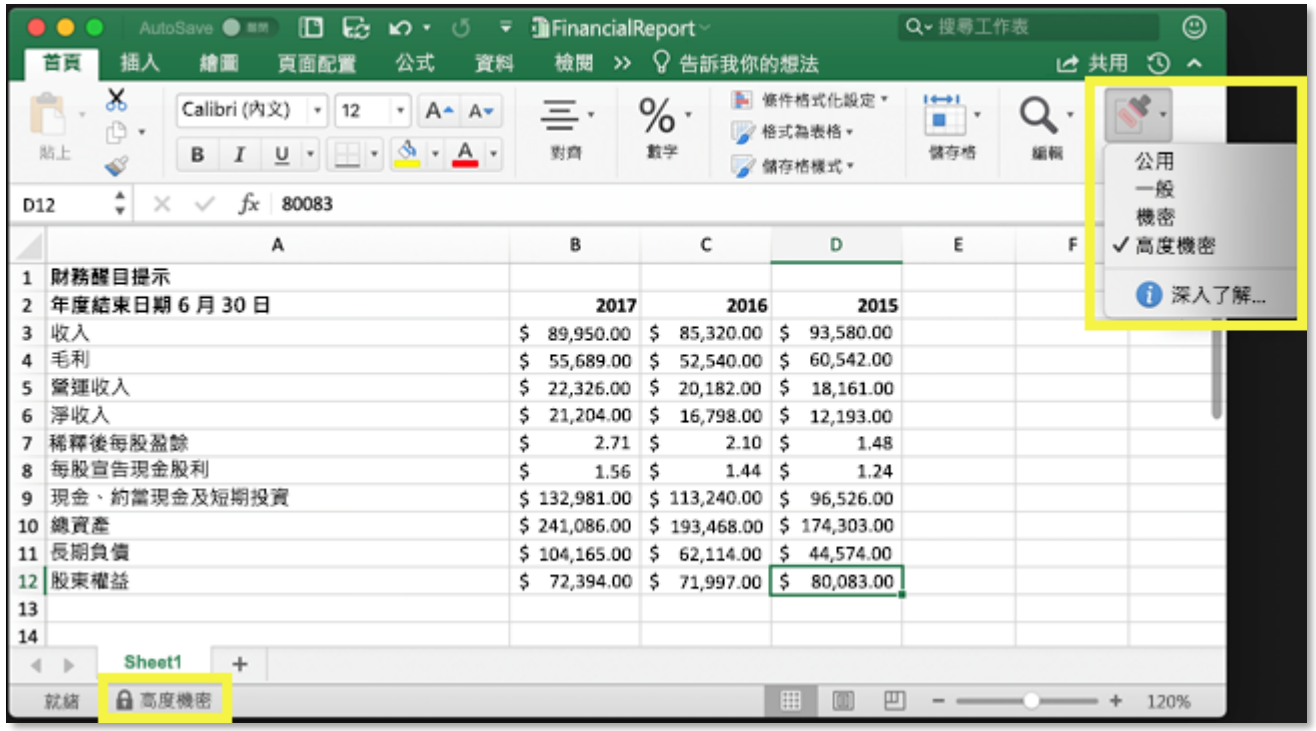
一、資料分類定義

二、存取控管與資料保護

三、資料追蹤與紀錄報告

#資料安全 -資料治理與加密

Azure Information Protection 透過資料探索與自動分類，並依分級進行對應的保護動作(e.g., 加密、浮水印)，達到集中治理目的



可整合應用場景

用戶端電腦裝置(Windows/Mac)

用戶端行動裝置(iOS/Android)

地端 Windows File Server

有支援SMB或NFS協定的設備 (e.g.,地端 NAS)

雲端檔案服務 (e.g., SharePoint Online)

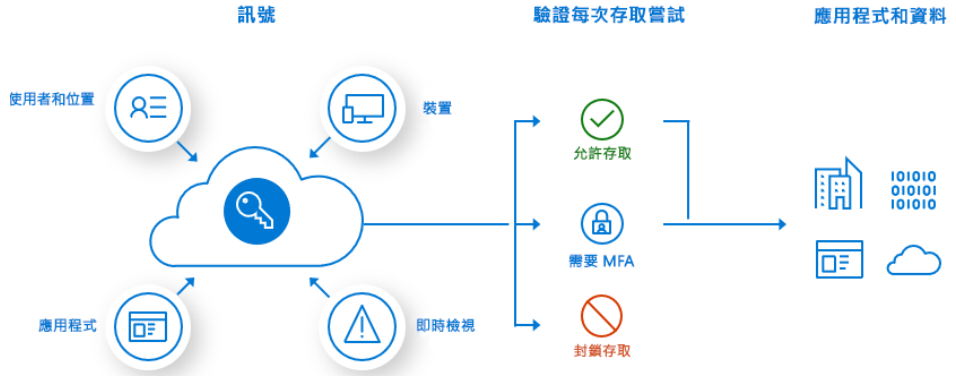
雲端郵件服務 – Exchange Online

資料外洩防護(DLP) – Windows 10端點

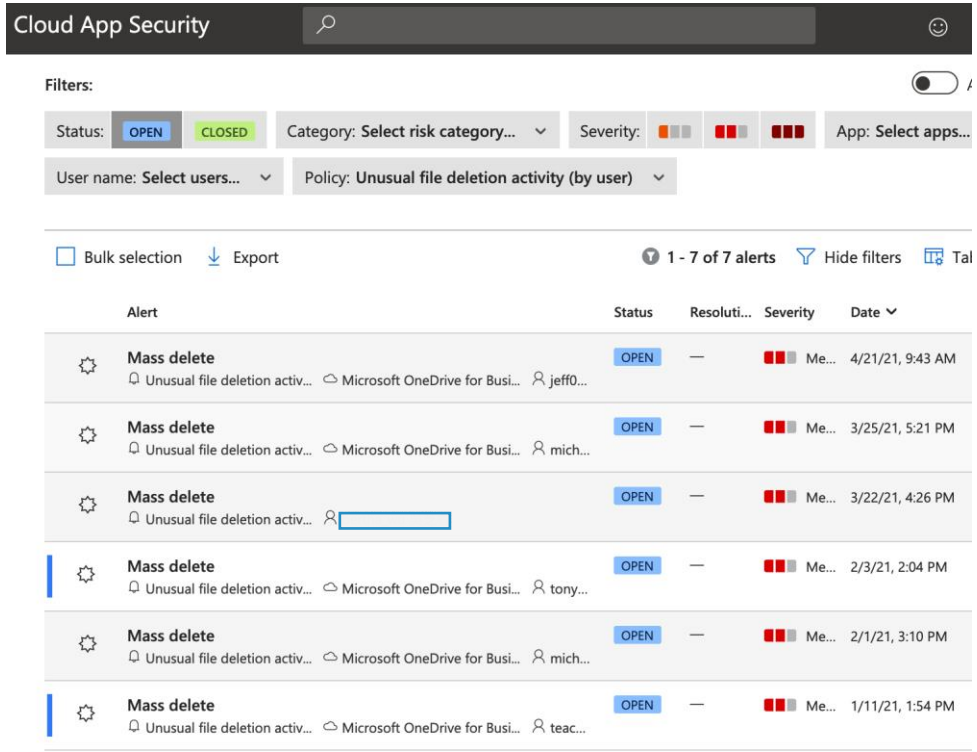
資料外洩防護(DLP) – Microsoft 365

#資料安全 –條件式存取

Azure AD 條件式存取



Microsoft Cloud App Security 針對雲端應用程式內的資料與操作行為進行控管，防範潛在威脅與異常狀況

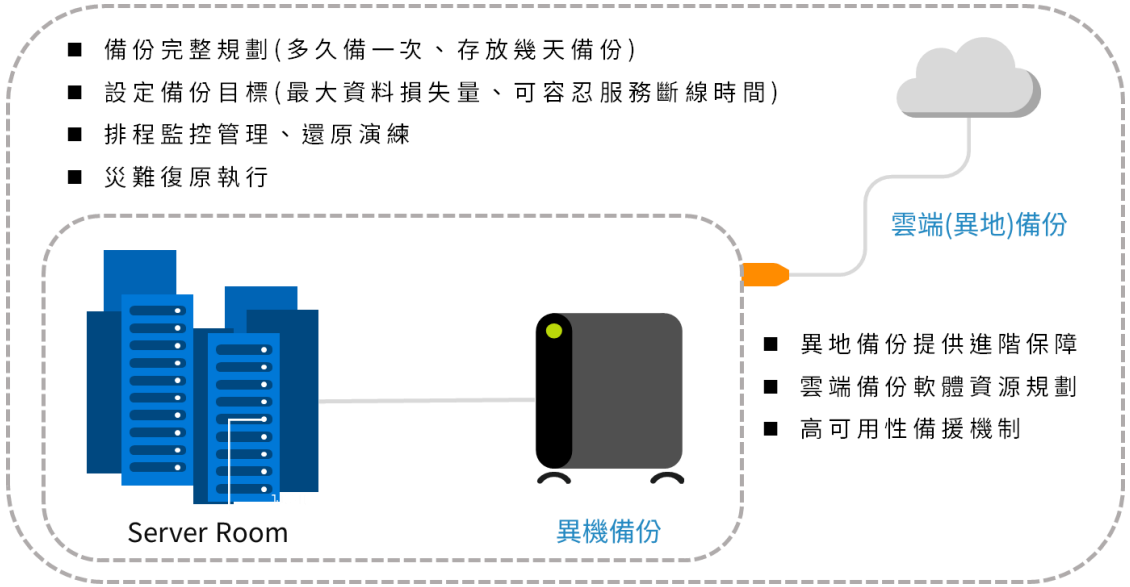


FREEDOM SYSTEMS

#資料安全 -備份與災難還原

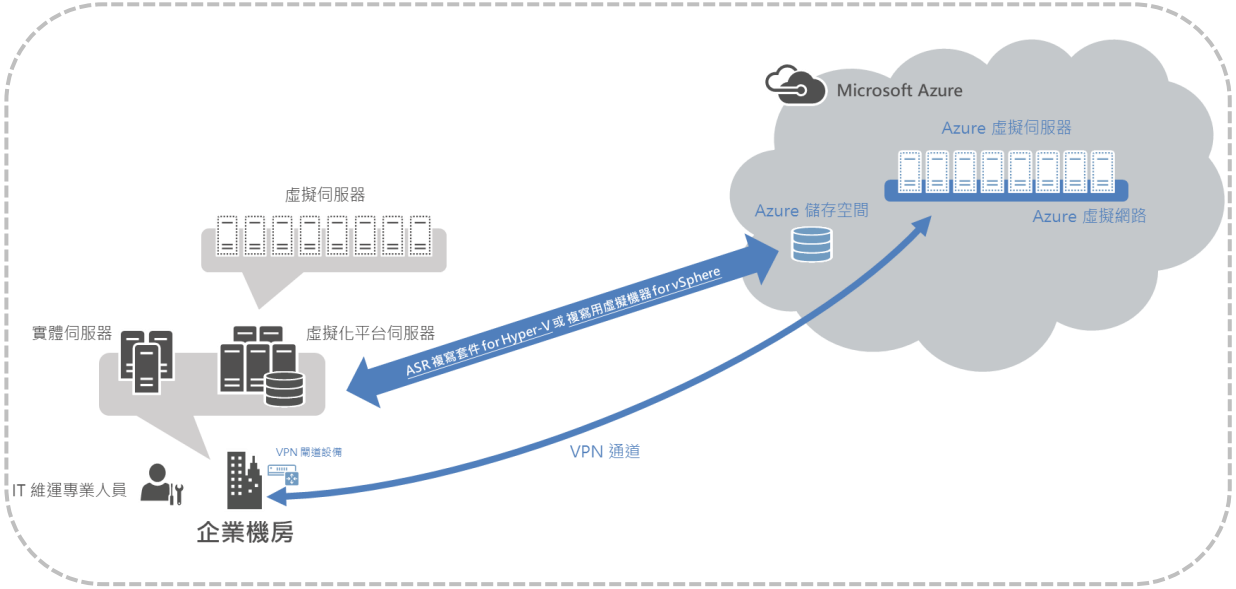
確實執行備份3-2-1原則 -3份資料 2個儲存媒介 1份在異地

搭配Azure Backup或第三方 (e.g., Veeam) 雲端備份方案



確實於雲端機房建立異地備援站台，鞏固災難發生時的可用性

搭配Azure Site Recovery或第三方 (e.g., Veeam)備援方案



FREEDOM SYSTEMS

資料安全防護顧問諮詢服務範圍

Enterprise Mobility+ Security (EMS)

Azure Active Directory (AAD)服務項目:
- 透過「**條件式存取**」強化雲端身分控管(MFA)
- 開發者與使用者可統一管理SaaS、SSO登入的平台

Azure Information Protection (AIP)服務項目:
- 協助「**檔案源頭性加密**」—套用敏感度標籤，針對資料進行自動分類及加密
- 與M365 Audit Log可針對檔案存取、分享足跡進行稽核與追蹤

Microsoft Cloud App Security 服務項目:
- 針對「**異常存取行為**」設立偵測警示原則，即時告警並阻斷異常行為
- 與AIP結合，追蹤檔案外流足跡

Microsoft Intune 服務項目:
- 協助Windows Autopilot Hybrid Domain Join
- IOS裝置前置設定
- Intune Device Management Setting
- Intune APP Management Setting
- 限定資料流動範圍

高級警示事件(非立即性攻擊)處理:
- 事件偵查與定義
- 依定義層級進行應變處理
- 提供調整建議

中級警示事件(非立即性攻擊)處理:
- 事件偵查與定義
- 依定義層級進行應變處理
- 提供調整建議

緊急攻擊事件回應及處理:
- 回應及遠端連線處理、到場處理
- 攻擊阻斷處理、災情控制應變
- 營運復原計畫及執行
- 攻擊源頭分析
- 漏洞修補與優化建議

定期告警事件檢視:
- 定期蒐集內部正常之事件回報並調整告警設定
- 第三方軟體事件統整及政策調整
- 警報通報機制建立與維護

自由系統的獨到之處與服務效益

即時且高效率地調查、遏制並修補重大資安事件

危機管理與即時應變

事件發生當下，沒有應對經驗的企業容易無所適從。您需要具有豐富處理經驗的團隊進場協助、主導陣營，能就事件相關的溝通事宜給予建議，包含與主管溝通、與IT及其他廠商協作。

蒐集調查威脅情報

若企業沒有資安團隊，往往當事件噴發時無法有效判讀威脅，也無從排除。專家就像解籤師，能透過工具比對數據紀錄、第三方資源等情報，進行有效率的調查、定義問題，找出攻擊的源頭。

以顧問式服務為本位

解決問題才是我們與客戶的共同目標。您不需要擔心廠商銷售不適用的產品，或是解決方案難以在組織落地。從問題洞察到技術維運全部交予一站式的服務，將資安管理納入企業永續經營方針。

專業解籤

判讀事件內容、定義緊急優先程度

即時處理

事件回應及應變處理

動態優化

環境結構調整、工具設定調整

FREEDOM SYSTEMS

資訊安全服務流程

Security Workshop
Estimated Time: 3-5 weeks

針對需求進行部分規模PoC Workshop

■ 工具測試佈署：
基本方案以 Microsoft Defender for Endpoint 及 Defender for Identity 為主要工具，可依照客戶需求調整配置與報價。

■ 資安健檢服務：
於3-5周內佈署後持續監控環境、處理告警並提交結果報告，如過程中發現重大資安漏洞將主動且即時通知客戶處理。

■ 方案價格：
- NT$ 約20萬 (Estimated Price)

(※依照企業部署規模與客製化程度不同，將影響報價)

Implementation
Estimated Time: 4-5 weeks

確認企業資安需求逐步導入資安產品

■ 完整導入解決方案：
依據Workshop結果報告與客戶溝通需求與現況，進行完整的資安架構規劃，以及完成產品佈署。

■ 佈署後監控與障礙排除：
完成Onboarding後，自由系統將進行短期的監控測試，以及障礙排除，確保工具上線後的正常運作。

■ 方案價格：
- 客製化報價，包含授權費用與專案費用

(※依照企業部署規模與客製化程度不同，將影響報價)

Managed Service
Estimated Time: Pay per mth

自由系統成為委外資安維運夥伴
以訂閱制服務 協助企業動態優化

■ 資安監控服務：
與客戶端協議監控範圍，以及所部署之工具定期監控，並參與定期會議報告

■ 資安改善建議：
定期根據 OS Patch、App Patch 等提交總體資訊環境或資安報告建議

■ 方案價格：
- 月訂閱或年訂閱制付費
- 客製化報價

(※依照企業部署規模與客製化程度不同，將影響報價)

※本項服務名目為Workshop，不含正式Implementation及Managed Service。詳細請洽自由系統。

FREEDOM SYSTEMS

自由系統資安服務客戶案例

Learn More→

研華在2020年底決定開始重新檢討既有資安管理，加強己身的資訊架構體質、降低被攻擊的風險，與縮短被攻擊後的反應時間。自由系統憑藉專業實力在眾多優秀Security Partners之中脫穎而出，成為研華的資安顧問，並分成三步驟確實進行資安健檢：1. 協助分析現況之風險，與現存之攻擊 2. 導入資訊安全工具，並提供資安維運服務3. 提出架構改善建議(AD、Email、Firewall)，並協助執行。

有察於地端server版本老舊，除了日常使用與維運問題，更擔心造成系統資安漏洞。自由系統的首要之務是協助艾訊評估比較升級地端server或上雲端的資訊成本、風險和生產效益，並規劃並執行地端email server移轉上雲端。除了Microsoft 365授權及導入，交給自由系統支援每月技術維運及教育訓練，更與微軟合作進行Security Workshop PoC，使用Microsoft Defender For Endpoint為艾訊降低端點資安風險。

台灣人壽為了因應大量資料處理，並有效從中發掘潛在資安事件，委託自由系統及微軟聯手抵禦資安潛在風險。導入Azure Sentinel後，藉由AI的高度學習及運算能力，以及視覺化的儀表板，將台灣人壽每日60十億位元組的資料，壓縮在半小時內檢視、回應及處理完成，協助內部資安人員更有效進行資源分配及利用。

為確保產業領先地位，瑞昱決心積極佈局資訊安全規劃，以降低經營風險及可能面臨的災損。自由系統透過佈署Microsoft Defender for Identity，優化企業內部的監控機制，若偵測到可疑的駭客橫向移動或攻擊行為，將可在第一時間示警並進行停權及環境檢查，搶在駭客發動更嚴重的攻擊前阻斷其動作。後期陸續使用Azure Security及Microsoft Defender來強化鞏固安全防護，也強化風險警示。

資訊安全與原廠合作認證

自由系統具有全球知名資訊安全組織(ISC)2的專業資格證照
提供的資安服務能更切身協助企業制定資安管理政策，評估風險範圍與有效控制

(ISC)²®

CISSP® | Certified Information Systems Security Professional

CISSP®認證被譽為資訊安全界的最高標準，偏重資安管理概念，主要訴求對象是中高階資安主管，例如CSO(安全長)、CISO(資安官)，或者是資安顧問等

SSCP® | Systems Security Certified Practitioner

SSCP®認證是針對具有資訊安全技術能力且具實務經驗者而設，此證照以公正客觀的標準，界定了企業組織中實際負責運作及落實資安政策相關從業人員的實務工作範圍、角色與職務

Microsoft Partner
Microsoft
Gold Security
Gold Cloud Platform
Gold Cloud Productivity
Gold Windows and Devices
Gold Small and Midmarket Cloud Solutions

Winner Microsoft Partner
2021 Partner of the Year
Taiwan
Microsoft

Hewlett Packard Enterprise Business Partner
Business Partner

cisco Select Partner

vmware PARTNER
PROFESSIONAL SOLUTION PROVIDER

veeam GOLD pro partner

DELL PartnerDirect Preferred

Adobe Certified Reseller

Symantec. Specialist Partner
Small and Midsize Business Segment

FireEye Product Specialist

(ISC)²國際資訊系統安全核準聯盟為非營利性的全球知名資訊安全組織，成立於1989年。
(ISC)²開發資訊系統安全核準認證計畫，並為資訊安全人員提供專業資格認證、教育及考試服務。(ISC)²的認證是一張保持中立、客觀的證照，獨立於任何軟體或廠商之外，(ISC)²頒發的專業人員認證受到全世界的認可(符合ISO/IEC 17024全球人才認證評估標準)

FREEDOM SYSTEMS

讓自由系統陪伴您成長，共同打造IT績效

IT is not an issue, call us!

FREEDOM SYSTEMS

自由系統股份有限公司 ©

02-2655-0668

sales@freedom.net.tw

www.freedom.net.tw