Exchange Online Protection (EOP)

1 反垃圾郵件保護

1.1 提供輸入垃圾郵件偵測
1.2 提供輸出垃圾郵件偵測
1.3 提供 NDR 退信攻擊保護
1.4 提供大宗郵件篩選
1.5 提供惡意 URL 封鎖清單
1.6 提供反網路釣魚保護

2 垃圾郵件管理方面

2.1 提供設定連線篩選 IP 允許清單與 IP 封鎖清單的功能
2.2 提供自訂每個使用者、群組或網域之內容篩選原則的功能
2.3 提供設定要對經過內容篩選的郵件所採取的動作之功能
2.4 提供設定進行嚴苛垃圾郵件篩選之進階選項的功能
2.5 提供國際垃圾郵件篩選
2.6 提供透過 Outlook 或 Outlook Web App (OWA) 管理垃圾郵件
2.7 提供透過 Microsoft Office Outlook 的垃圾郵件回報增益集提交垃圾郵件
2.8 提供透過電子郵件別名提交垃圾郵件和非垃圾郵件
2.9 提供透過 OWA 垃圾郵件回報提交垃圾郵件和非垃圾郵件
2.10 提供使用者垃圾郵件隔離通知
2.11 提供讓系統管理員設定使用者垃圾郵件隔離通知語言的功能
2.12 提供透過網頁存取和管理隔離區中的郵件
2.13 提供搜尋隔離的功能
2.14 提供從 Exchange 系統管理中心檢視垃圾郵件隔離郵件標頭

3 反惡意程式碼保護方面

3.1 提供多重引擎反惡意程式碼保護
3.2 病毒偵測和封鎖 SLA 100% 已知病毒
3.3 提供停用惡意程式碼篩選的選項
3.4 提供郵件內文及附件的惡意程式碼檢查
3.5 提供預設或自訂惡意程式碼警示通知
3.6 提供偵測到惡意程式碼時移除附件的選項
3.7 提供反間諜軟體保護
3.8 提供自訂每個使用者、群組或網域之惡意程式碼篩選原則的功能

4 其他功能

4.1 異地備援的伺服器全域網路
4.2 內部部署伺服器無法接收郵件時，將郵件加入佇列

Office 365 進階威脅防護 (ATP)

1 提供安全連結-ATP

安全連結功能主動保護使用者，抵禦郵件中的惡意超連結。因為可動態封鎖惡意連結，允許存取無害連結，每次使用者按一下連結時都能受到持續保護。

2 提供安全附件

安全附件可防止不明的惡意軟體和病毒，並提供零時差保護來保護郵件系統。所有沒有已知病毒/惡意軟體簽章的訊息與附件將被路由傳送至特殊的環境，其中 ATP 會使用不同的機器學習與分析技術來偵測惡意的意圖。如果未偵測到可疑活動，即會釋出訊息傳遞到信箱。

3 提供詐騙智慧

詐騙智慧偵測時寄件者看起來會將代表一個或多個使用者帳戶的郵件傳送內的其中一個貴組織的網域。系統可允許檢閱所有寄件者詐騙的網域，然後選擇允許繼續或封鎖的寄件者。

4 提供隔離區

由 Office 365 服務識別為垃圾郵件、大量郵件、網路釣魚郵件、包含惡意程式碼的郵件，或因為它們符合郵件流程規則的郵件都可以傳送至隔離區。根據預設，Office 365 會直接將網路釣魚郵件和包含惡意程式碼的郵件傳送至隔離區。經過授權的使用者可以檢視、刪除或管理已傳送至隔離區的電子郵件郵件。

5 提供進階反網路釣魚功能-這項功能會使用機器學習模型來偵測網路釣魚郵件。

6 適用於 SharePoint、 OneDrive 及 Microsoft Teams ATP:會保護組織，當使用者共同作業和共用檔案，藉由識別和封鎖惡意檔案小組網站和文件

7 威脅調查及回應功能

7.1 威脅追蹤器

提供最新智慧主流 cybersecurity 問題。可以檢視最新惡意程式碼的相關資訊，並採取的因應對策之前就會變成組織實際威脅。 可用的追蹤器包括值得注意的追蹤器、趨勢追蹤器、追蹤查詢，以及已儲存查詢。

7.2 威脅瀏覽器

使用威脅檔案總管分析威脅，攻擊數量一段時間及分析的威脅系列、 攻擊者基礎結構及其他資料。

7.3 自動化的調查及回應功能

可調查潛在的網路攻擊，可以用最少的時間與更快速地找出威脅，並降低對企業/組織/員工的影響

7.4 Office 365 中的攻擊模擬器

可以在組織中執行真實的攻擊案例使用攻擊模擬器，目前可用的三種類型的攻擊模擬包括:顯示名稱矛網路釣魚攻擊、密碼噴灑攻擊、暴力密碼攻擊，協助找出並尋找容易遭受使用者之前真實的攻擊影響