Weblink Microsoft Defender Consulting Services

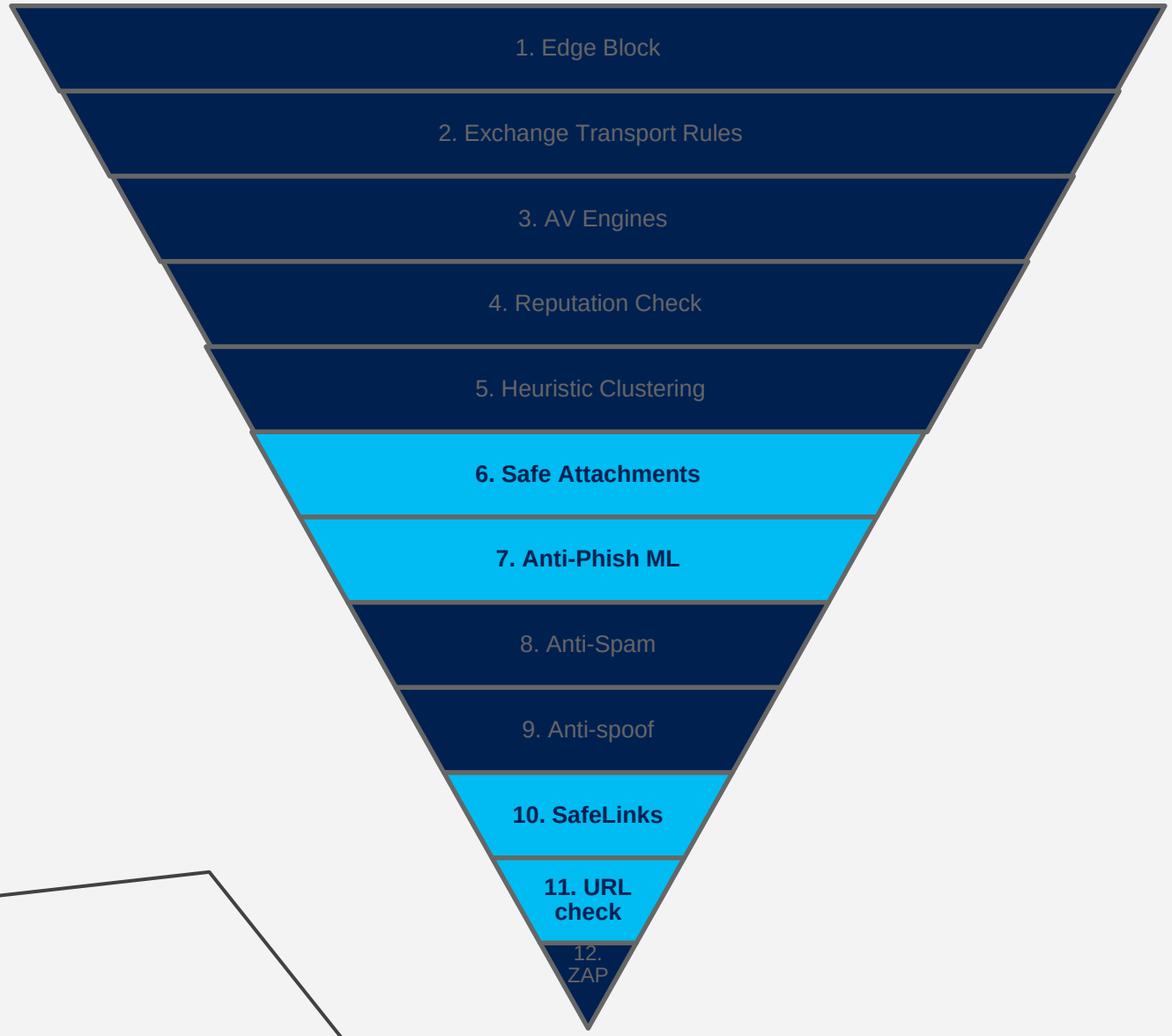
Microsoft Defender for Office 365

- Microsoft Defender for Office 365 是一項電子郵件篩選服務，可幫助防止不安全的連結和附件，同時提供強大的追踪和報告功能。
- Microsoft Defender for Office 365 基於 Exchange Online Protection（EOP），使用先進的機器學習技術和隔離的引爆室來捕捉最新的惡意軟體。

Microsoft Defender for Office 365

- Microsoft Defender for Office 365 可用於以下三種方案：
  - Exchange Server 環境或任何其他本地式 SMTP 電子郵件解決方案, 提供雲端式電子郵件保護
  - Exchange Online 的雲端託管信箱
  - Exchange 混合部署

Microsoft Defender for Office 365 架構概觀



EOP / ATP 使用 “漏斗方式” 進行保護 , ATP技術是淺藍色的。 EOP 階段過濾掉很多郵件，因此 ATP 執行效率更高.

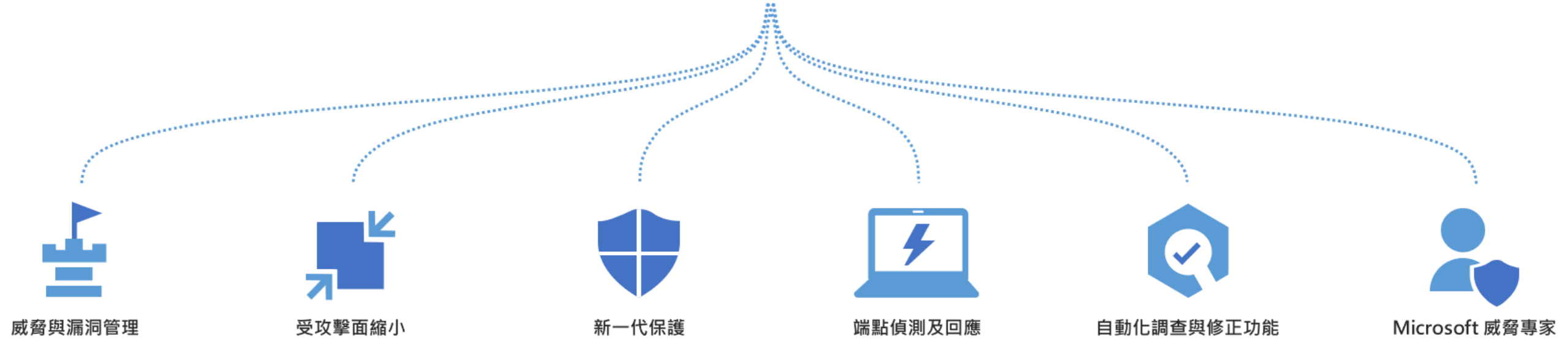
1. EOP -最明顯的惡意軟體在邊緣被阻止； 查看IP /發送方信譽等.
2. EOP -Exchange Transport Rules (ETRs) – 執行特定的公司法規和政策，以及如何使用稽核報告來追蹤服務的設定變更.
3. EOP – 防毒引擎 – 基於多引擎防禦已知威脅的簽章.
4. EOP – 信譽檢查 -來自引爆 (#5) and 1st (包括 MDATP) and 3rd 提要. 創新威脅通常在這裡被阻止.
5. EOP – 啟發式叢集 -檢查所有郵件流程尋找未檢測到的惡意軟體模式, 當達到閾值時,它將主動將文件發送到沙箱引爆。 然後,將確認的錯誤文件雜湊值增加到上游信譽快取(#4).
6. ATP – 安全附件 –原則範圍內所有附件基於原則的引爆
7. ATP -反網路釣魚機器學習
8. EOP – 反垃圾郵件
9. EOP – 反詐騙 – 檢測內部使用者的詐騙，如果發件人不符合正常模式，則通知收件人.

10-11. ATP –安全連結和URL信譽檢查– 對電子郵件和文件中URL的點選即時保護.

12. ZAP – 交付後保護，如果在交付後進行檢測，則從收件箱中刪除未讀的惡意軟體.

Microsoft Defender for Endpoint

Built-in. Cloud-powered.



Microsoft Defender for Endpoint

- **威脅與漏洞管理**
  這個內建功能使用遊戲變更的風險方法，來探索、確定及修正端點漏洞和錯誤配置。
- **受攻擊面縮小**
  「攻擊」表面減少的功能集合提供堆疊中的第一個防線。 透過確保設定正確地設定設定並套用利用緩解技術，這些功能可抵禦攻擊和利用。 這組功能也包括網路保護和 Web 防護，控管對惡意 IP 位址、網域和 URL 的存取。
- **新一代保護**
  為了進一步鞏固您網路的安全性周長，Microsoft Defender ATP 會使用下一代保護，以捕捉所有類型的新興威脅。
- **端點偵測及回應**
  端點偵測及回應功能可讓您偵測、調查及回應前兩個安全支柱所帶來的高級威脅。 [先進式搜尋] 提供以查詢為基礎的威脅搜尋工具，可讓您主動找出違規行為並建立自訂的檢測。
- **自動化調查與補救措施**
  為了同時搭配快速回應進階攻擊的能力，Microsoft Defender ATP 提供自動化調查與補救功能，協助在幾分鐘內大幅減少警示數量。
- **Microsoft 威脅專家**
  Microsoft Defender for Endpoint 的新受管理威脅搜尋服務提供主動的搜尋、優先順序及其他內容與深入見解，進一步讓安全性作業中心（SOCs），以快速且準確地識別及回應威脅。

Microsoft Defender for Identity

Microsoft Defender for Identity 作為地端和雲端環境的一部分，可幫助安全營運團隊保護使用者身份。

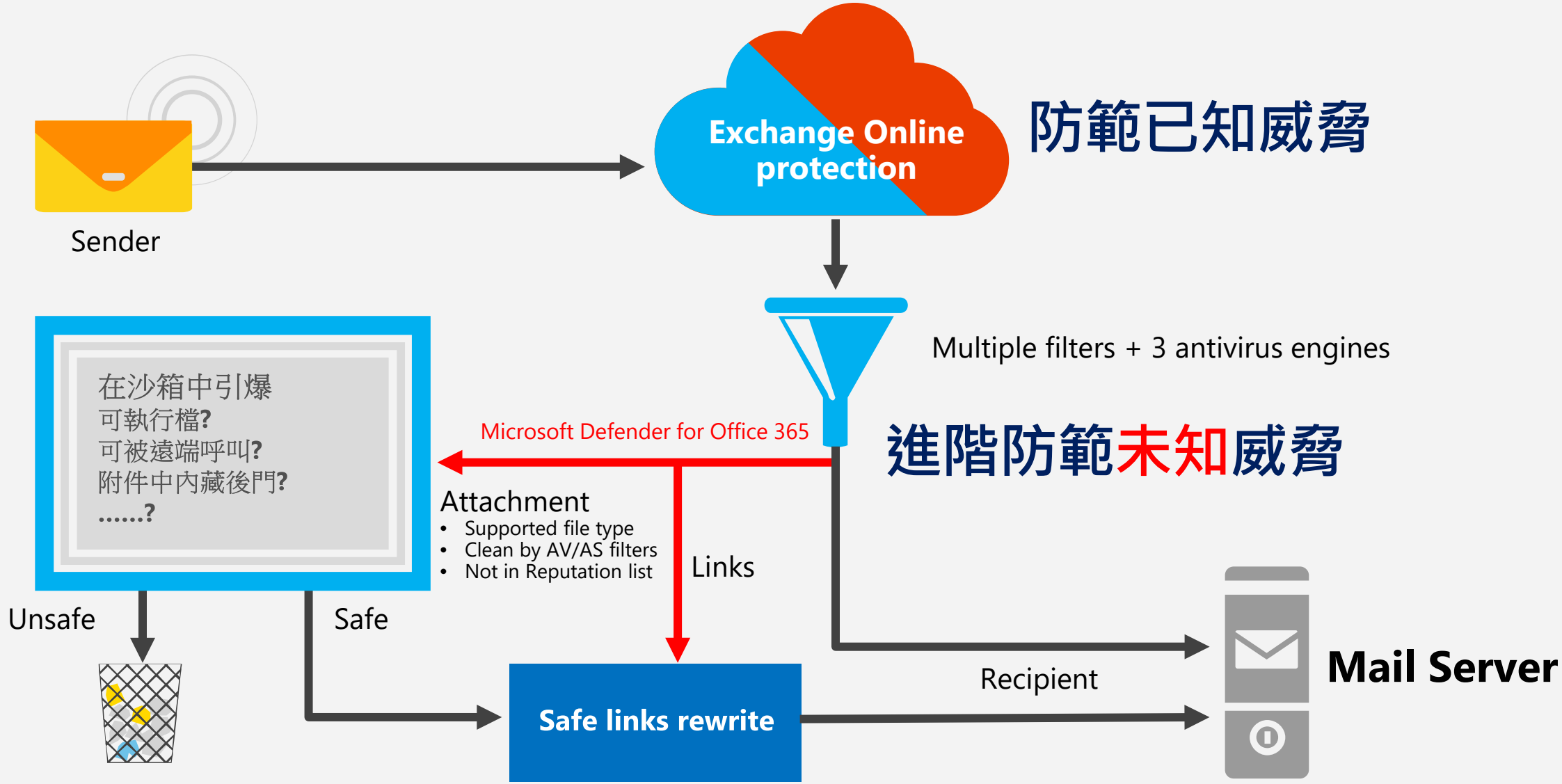
Microsoft Defender for Identity

Microsoft Defender for Identity 提供無與倫比的情報和即時分析功能，使其成為地端身份安全性的最佳選擇。

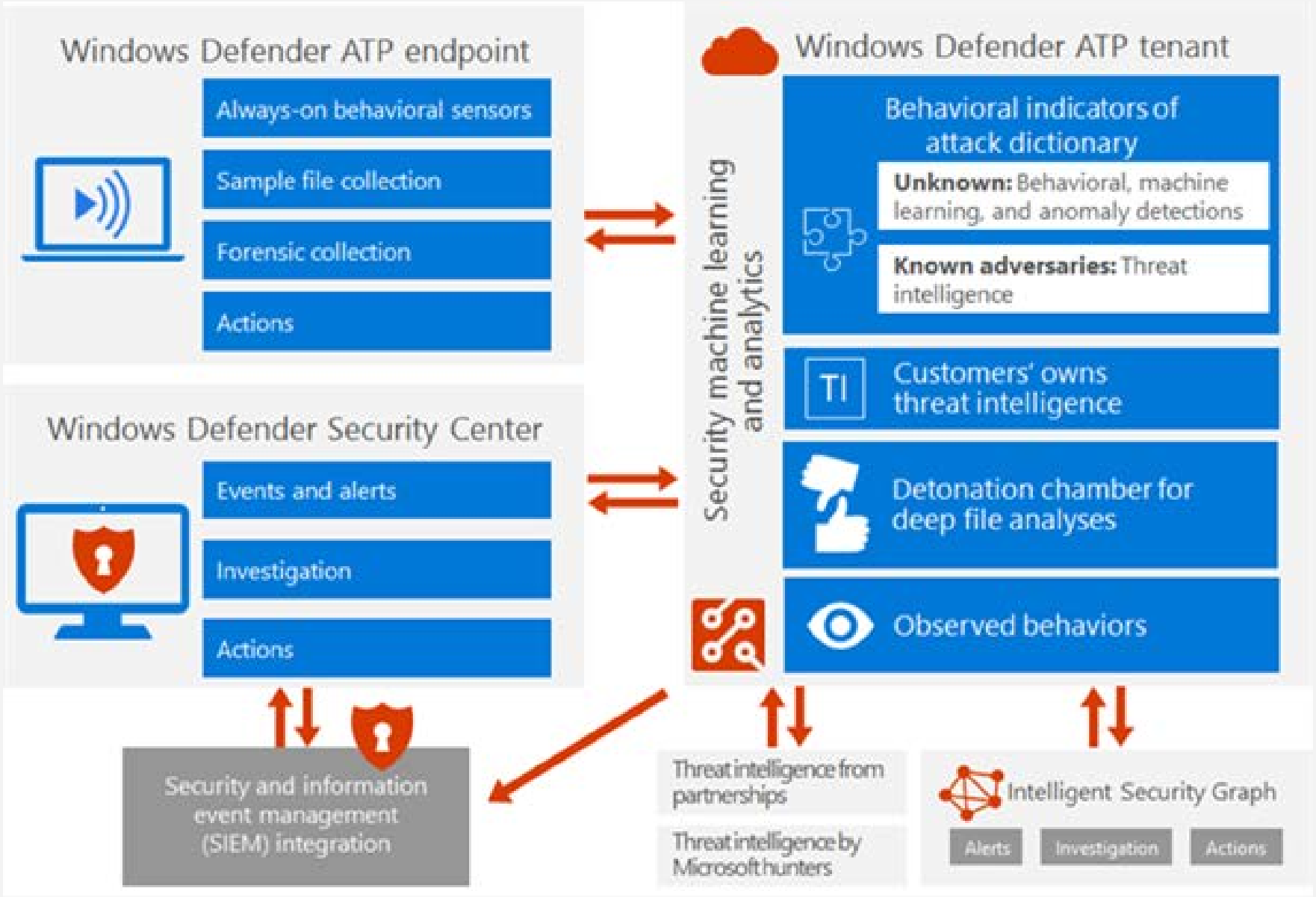
Microsoft Defender for Identity 與 Microsoft Cloud App Security 和 Azure AD Identity Protection 集合在一起，是整體 Microsoft Threat Protection 方案。

獲取一流的產品和無與倫比的方案　提供卓越的威脅防護。

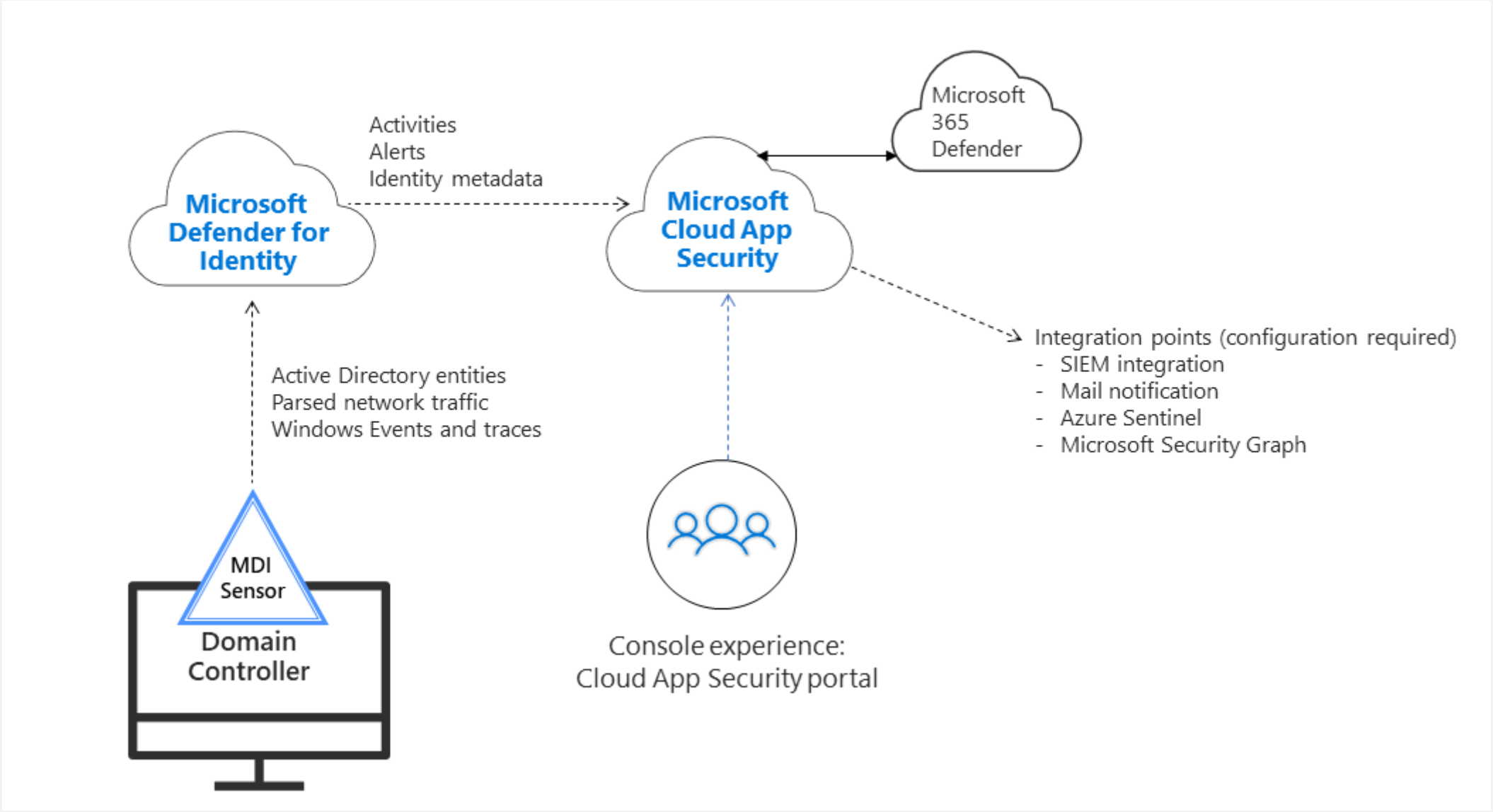
Microsoft Defender for Office 365 架構圖



Microsoft Defender for Endpoint 架構圖



Microsoft Defender for Identity 架構圖



Thank you