透過 XDR 增強您的 SecOps 成效

使用 Microsoft Defender 全面偵測回應 (前身為 Microsoft 365 Defender)，在網路攻擊鏈中取得事件層級可見度，透過自動中斷進階網路攻擊和跨端點和 IoT、混合式身分識別、電子郵件和共同作業工具、軟體即服務 (SaaS) 應用程式、雲端工作負載和資料的加速回應，將 SOC 團隊提升到一個新水準。

端點

探索並保護您多平台企業上的端點和網路裝置。

身分識別

管理和保護混合式身分識別，並賦化員工、合作夥伴和客戶的存取。

SaaS 應用程式

取得可見度、控管資料，以及偵測雲端服務和應用程式中的網路威脅。

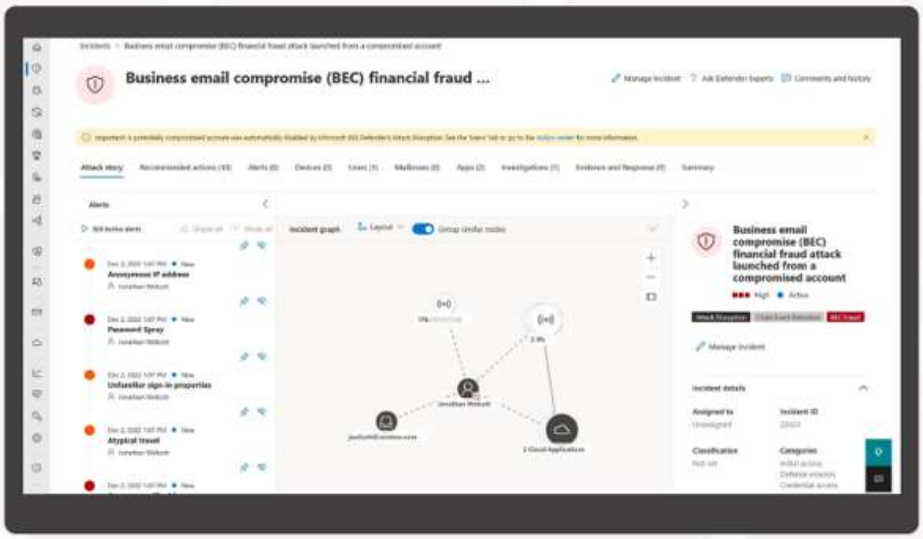
電子郵件和共同作業工具

保護您的電子郵件和共同作業工具，以防範網路釣魚和商業電子郵件入侵等進階網路威脅。

Microsoft Defender 全面偵測回應重要功能

使用 XDR 整合安全性。

- 以電腦速度自動中斷進階網路攻擊
- 使用以 XDR 為優先的事件啟用快速回應
- 使用 Microsoft Security Copilot 重新塑造 SOC 生產力
- 自動修復受影響的資產
- 主動搜捕網路威脅
- 更有效地管理多租用戶環境



以電腦速度自動中斷進階網路攻擊

使用 AI 阻止進階網路攻擊 (例如勒索軟體) 的橫向移動，儘早限制網路攻擊者的進展，並讓 SOC 團隊完全控制調查及補救網路威脅。

深入了解 >