益處

- 透過詳盡而可行的報告與分析，在您的環境中達成能見度與控管功能。
- 為您的安全分析人員建立可採取動作的情報（包括追溯性安全情報）
- 整合端點所需的進階惡意軟體保護和現有的安全性程序
- 在參與過程中透過知識傳授，確保您的員工具備執行解決方案的技巧
- 針對不同部門量身打造防護設定檔
- 妥善運用廠商的最佳實務，以符合該解決方案的內部和外部稽核需求

端點部署適用的思科 AMP

防範入侵網路末端的惡意軟體

即使您已在所有門戶裝置了最佳防護，還是需要內部的防護措施。而這正是適用於端點的思科® 進階惡意軟體保護 (AMP) 能提供的服務。防範入侵能在罪犯試圖入侵網路之際予以攔截，不過這只適用於傳入通訊，而且是只有一次攔截機會的評估方案，一旦錯失之後，就無法再看見入侵的事物。如果通過門戶的是惡意軟體，那該怎麼辦呢？

AMP 是唯一能在攻擊之前、期間以及之後提供涵蓋所有端點的進階惡意軟體保護系統，並能持續進行資料收集和進階分析。透過使用這些資訊以及思科追溯性安全工具（例如追溯、攻擊鏈關聯性、危害的行為指標、軌跡以及找出入侵），安全經理得以回顧威脅發生的時間點。您可以追蹤過程、檔案活動與通訊，瞭解感染的範圍，確定根本原因並執行補救措施。

端點部署服務適用的思科進階惡意軟體保護 (AMP) 能協助您成功安裝此防護功能。我們會在 45 天內部署、設定、測試，以及初始調整多達六 (6) 個端點群組內的實作，並且採用思科最佳實務，協助您避免可能耽誤部署作業、增加成本並可能導致您的網路處於未保護狀態的種種錯誤。

迅速啟動並執行防護

規劃並實施部署不僅相當快速，也十分完善。以下是我們在部署之前、期間以及之後所採取的步驟。

部署前

- 執行遠端啟動通話與專案計畫檢查，找出主要利益關係人，並提供專案管理計畫（包含活動的時間表及排程）
- 根據網路拓撲檢視、資產分類、目前的技術設定與防護狀態，提供部署及設定建議
- 檢視客戶的資訊安全、資訊技術、變更控制原則和物料清單
- 檢視部署、策略、設計與設定的最佳做法

部署

- 定義適用於端點的 AMP 之原則
- 識別初始 Alpha 版部署端點
- 透過預先定義指定數量的端點連接器，針對適用於端點的 AMP 之 Alpha 版部署，進行部署、設定、初始調整及驗證
- 找出優先順位的端點，提供限定數量的生產部署
- 為多達六個端點群組執行一個連接器套件推送

部署後

- 在部署後大約 30 天，驗證限定數量的生產部署的效能，並提供遠端附加最佳化調整
- 根據適用於端點的 AMP 分析元件之使用方式傳授相關知識
- 提供並檢查部署摘要報告 (DSR) 中關於部署適用於端點的 AMP 之摘要資訊

端點部署適用的思科 AMP 提供兩種銷售版本：最多 5000 台裝置或最多 25,000 台裝置的部署，並可自訂範圍，以符合您的特定需求。

後續步驟

如需詳細資訊，請造訪 www.cisco.com/go/services/security。

C45-734143-00 09/16