思科 AMP 終端版

找出您長久以來遺漏的的 1% 威脅

市面上幾乎所有端點解決方案都聲稱能封鎖 99% 的惡意軟體，但遺漏的 1% 威脅又該如何阻擋？這 1% 的威脅會讓您的網路天翻地覆。如果您只採用防毒軟體等傳統的時間點防護技術，那麼威脅可在您偵測不到的情況下潛伏數個月。

保護使用者的安全比以往更加重要

組織內越來越多員工使用行動裝置，工作模式也更具彈性。員工可使用筆記型電腦、平板裝置或手機等各種裝置登入或登出公司網路，隨時保有生產力。網路架構現已設計成允許遠端存取，甚至可存取高度敏感資料。

可惜的是，攻擊者也越來越善於掌握這樣的趨勢；而且還會利用專為繞過傳統型端點資安工具而設計的威脅，鎖定員工及其裝置上有價值的重要資料。企業要如何在持續創新、進行數位轉型，並讓員工使用行動裝置辦公的同時，又不犧牲安全性呢？

新世代端點安全

新世代端點安全運用雲端分析的強大威力，將防護、偵測和回應功能整合在單一解決方案中。思科® AMP 終端版是輕量型連接器，能在 Windows、Mac、Linux、Android 和 iOS 裝置上運作；且可使用公共雲或部署為私有雲。AMP 可持續監控和分析所有檔案，並處理網路內的活動，進而找出其他解決方案忽略的 1% 威脅。AMP 不會遺失檔案的去向，也會密切追蹤檔案活動。如果檔案的初期偵測結果未受到感染，但卻出現惡意行為，AMP 會有威脅行為的完整記錄，可讓您迅速攔截、遏制和修復。

優勢

思科® AMP 終端版提供全方位的防護，可抵禦進階型攻擊；且能在攻擊作業和惡意軟體入侵當下進行防範並加以封鎖，然後快速偵測、遏制及修復可規避前線防禦機制並進入網路的進階威脅。

- **預防：**使用最優異的全球威脅情報鞏固防禦，並即時封鎖無檔案型及檔案型威脅。
- **偵測：**持續監控並記錄所有檔案活動，以快速偵測隱匿的惡意軟體。
- **回應：**加速調查並自動修復 PC、Mac、Linux、伺服器和行動裝置（Android 和 iOS）中的惡意軟體。

後續步驟

諮詢思科銷售代表或通路合作夥伴，瞭解思科 AMP 終端版如何協助您保護組織，抵擋進階網路攻擊。請造訪我們的網站深入瞭解。

C45-731874-12 04/18

阻擋惡意軟體

AMP 終端版採用雲端型威脅情報及檔案分析。AMP 雲端會持續提供來自思科 Talos 與 Threat Grid 的資訊摘要，其相當於業界最龐大的即時威脅情報摘要集合。此雲端式作法能讓 AMP 根據最新的威脅情報分析檔案，進而防止現今不斷演化的惡意軟體入侵。

由於沒有任何一種方法能單獨阻擋惡意軟體，因此，AMP 提供了超過 15 種內建防護及偵測機制，防範威脅入侵您的企業網路；其中包括可阻止勒索軟體的惡意活動防護、無檔案型惡意軟體入侵防禦、分析新興威脅的機器學習技術、沙箱等等。即使檔案安然通過所有機制的檢查，AMP 允許檔案進入後，仍會持續監控及分析其是否出現惡意行為。

消除盲點

無論您採用哪一套作業系統，思科 AMP 終端版均可讓您零死角檢視端點。針對無法部署連接器的連線物聯網 (IoT) 裝置（包括印表機、恆溫器和監視攝影機），AMP 亦可提供異常流量的能見度。

思科知道網路犯罪極少只從一個攻擊向量出擊。因此，AMP 終端版會提供整個環境的威脅情報，並整合端點、網路、電子郵件、雲端及網路的安全性。透過這些整合，AMP 即可辨識出環境中某區域的威脅，當威脅出現在其他地方時便會自動將其封鎖。AMP 可自動相互關聯檔案、遙測資料、行為及活動，並主動防禦來自所有潛在向量的進階威脅。

探索未知威脅

AMP 的內建沙箱技術能分析可疑檔案的行為，並將其與其他資訊來源相互關聯。檔案分析可產生詳細資訊，讓您進一步瞭解如何遏制疫情擴散並阻擋未來的攻擊。

檔案歸為惡意檔案後，AMP 可大幅減少調查所需的時間和資源；且能自動提供最重要問題的深入分析，包括：

- 發生什麼事？
- 惡意軟體來自何處？
- 惡意軟體觸及哪些地方？
- 惡意軟體正在進行什麼活動？
- 如何加以阻止？

只要在 AMP 瀏覽器管理主控台中按幾下按鈕，即可封鎖檔案，避免其在所有端點上執行。思科 AMP 知道檔案觸及的所有其他端點，因此能為所有使用者隔離檔案。有了 AMP，即可精確修復惡意軟體，而不會對 IT 系統或業務造成連帶損失。