

ENTERPRISE THREAT PROTECTOR

雲端內的目標式威脅防護



企業遭受威脅的態勢正在快速演變。惡意軟體、勒索軟體、資料竊取，與網路釣魚等目標式威脅的數量與日俱增，惡意攻擊者規避傳統資安措施的能力也變本加厲。加上企業紛紛採用 SaaS、雲端與物聯網的狀況下，手法更老練的威脅傳遞方式已引發不容忽視的新挑戰、控制點複雜性以及安全落差。借助於 Akamai 綜觀網際網路與網域名稱系統 (DNS) 全局的精闢獨到見解，Enterprise Threat Protector 能使安全團隊得以主動封鎖及緩解目標式威脅，並在整個企業上下執行正當使用原則。

ENTERPRISE THREAT PROTECTOR

Enterprise Threat Protector (ETP) 建立於 Akamai Intelligent Platform™ 與 Akamai 的 AnswerX™ 電信級遞迴式 DNS 之上，是可以快速設定並且輕鬆部署的雲端解決方案，不需要部署或維護硬體或軟體。

憑藉著即時的 Akamai Cloud Security Intelligence，以及 Akamai 經過實證、遍佈各地的遞迴式 DNS 平台，Enterprise Threat Protector 得以主動辨識及封鎖惡意軟體、勒索軟體、DNS 資料竊取，與網路釣魚等目標式威脅。Akamai 的雲端入口網站讓安全團隊在短短數分鐘內就能針對所有員工進行集中管理，並執行一致的安全原則與正當的使用原則。

運作方式

網域名稱系統 (DNS) 是所有網際網路服務的基礎，許多惡意網域看準這點 (包括代管惡意軟體與勒索軟體的網站，以及相關的指揮與控制 (CnC) 伺服器)，便利用遞迴式 DNS 進行攻擊。

然而當企業的外部遞迴式 DNS 流量導向到 Akamai 的 Enterprise Threat Protector 時，系統會將要求的網域與 Akamai 的即時網域風險評分威脅情報進行比對，企業便能主動出擊，阻止員工存取惡意的網域與服務。因為這項驗證作業是在 IP 連線建立之前進行，所以能在安全攻擊鏈中早先一步阻止威脅，將威脅拒於企業門戶之外。此外，因為 DNS 的效用廣泛，遍及所有連接埠與通訊協定，從而能夠防範不採用標準網頁連接埠與通訊協定的惡意軟體。

系統也能檢查網域，判斷員工嘗試存取的內容類型，若內容違反企業的正當使用原則 (AUP)，即封鎖網域。

Enterprise Threat Protector 能輕易與其他安全產品和報告工具整合，包括安全網頁閘道、新一代防火牆、SIEM，以及外部威脅情報來源，讓企業能最大化他們在層層安全堆疊中所挹注的投資。

企業可享有的優點

- 大幅提升安全防衛能力：依據獨家最新的威脅情報，主動封鎖連往惡意軟體與勒索軟體網站、惡意軟體指揮與控制 (CnC) 伺服器的 DNS 要求，並阻絕 DNS 資料竊取行為和網路釣魚網域。
- 以不複雜且免硬體的方式立即增加防護能力：歸功於數分鐘內就能完成設定與部署 (不中斷使用者)，並能快速調整規模的 100% 雲端式解決方案。
- 輕鬆縮短管理時間：從任何地點，在數秒內就能管理安全原則與更新，以保護所有據點。
- 快速且一致地落實合規性與您的正當使用原則：封鎖令人反感或不當之網域與內容類型的存取權限。
- 立即提高 DNS 的彈性與可靠度：採用 Akamai 電信級全球情報平台。

ENTERPRISE THREAT PROTECTOR

AKAMAI CLOUD SECURITY INTELLIGENCE (CSI)

Enterprise Threat Protector 以 Akamai 的 Cloud Security Intelligence 為後盾，可提供惡意網域的即時相關情報，以及這些網域對企業帶來的風險。

相關情報是由 Akamai Intelligent Platform 每天收集的資料匯集而成 (Akamai Intelligent Platform 每天管理高達 30% 的全球網路流量，且遞送多達 1500 億筆 DNS 查詢)。加上外部的威脅消息來源，Akamai 情報系統又再獲得更進一步的強化。這些統合的資料集合會經由先進的行為分析方式進行分析。所得結果交由專屬的威脅研究團隊再做進一步加強。新威脅一經認出，便會立即新增到 ETP 服務，為企業及其員工提供即時保護。

AKAMAI INTELLIGENT PLATFORM

Enterprise Threat Protector 服務建立在 Akamai 的 Intelligent Platform 之上，該平台安全可靠、穩定快速。由於遍佈各地，該平台能夠實現 100% 可用性 SLA，並確保企業的遞迴式 DNS 服務具有最佳可靠度。

雲端型管理入口網站

Enterprise Threat Protector 的所有組態與當前管理，均是透過 Akamai 的雲端型 Luna 入口網站來執行，讓管理作業隨時隨地都能進行。

原則管理作業既快速又簡單。變更在數分鐘內就能推送至全域，確保所有企業據點與員工都受到保護。您可以設定電子郵件警告，讓安全團隊掌握重大的原則事件，並立即採取補救步驟，快速找出潛在的威脅並予以解決。即時儀表板提供 DNS 流量、威脅事件與 AUP 活動的概觀。任何活動的詳細資訊只要深入檢視個別的儀表板元素，就能查看。這份詳細資訊會提供寶貴的資源，以供分析及補救資安事件。

入口網站的所有功能均可透過 API 存取，DNS 資料記錄也可匯出到 SIEM，讓 Enterprise Threat Protector 能夠輕鬆且有效地整合您其他的安全解決方案與報告工具。

主要功能

- Akamai 歸類的威脅：最新的威脅情報可以詳細到以分鐘計算，歸功於 Akamai 所掌握的每日 15% 至 30% 網路總體流量，並結合 Akamai 遞迴式 DNS 雲端每日收到的 1500 億筆查詢。
- 由客戶歸類的威脅：安全團隊能迅速整合現有的威脅情報來源，從您現有的安全投資延伸出更多價值。
- 正當使用原則：限制哪些內容類型可以存取以及哪些不得存取，以執行企業的正當使用原則，並確保原則受到遵循。
- 分析與報告：儀表板能提供企業所有向外 DNS 流量、威脅與 AUP 事件的即時深入解析。
- 記錄：DNS 記錄會保留七天，而且可輕易匯出為 .CSV 檔案，或整合到 SIEM 中，供進一步分析。
- DNSSEC (域名系統安全延伸)：傳送到 Enterprise Threat Protector 的所有 DNS 要求，均已啟用 DNSSEC。

Akamai 價值鏈體系

Akamai 讓網際網路變得快速、可靠又安全。我們的全方位解決方案是以遍及全球的 Akamai Intelligent Platform™ 為基礎打造而成，透過可自訂的整合式 Luna Control Center 進行管理，方便您洞悉與掌控一切；此外，更有 Professional Services 的專家提供支援，讓您能夠輕鬆上手，並隨著您的策略發展激勵創新。



關於 Akamai

Akamai 為全球最大且最受信賴的雲端遞送平台，協助客戶以更輕鬆的方式隨時隨地在任何裝置上提供最優秀、最安全的數位體驗。Akamai 於 130 個國家或地區設置逾 200,000 部伺服器，以規模無人能及的龐大分散式平台為客戶提供優越效能與威脅防護。Akamai 的產品組合包括網站與行動效能、雲端安全、企業存取及視訊遞送解決方案，全都享有卓越的客戶服務與 24 小時全年無休的監控支援。想瞭解為何頂尖金融機構、電子商務大廠、媒體和娛樂供應商及政府機構均信賴 Akamai，歡迎瀏覽 www.akamai.com、blogs.akamai.com 或在 Twitter 追蹤 @Akamai。您可以在 www.akamai.com/locations 找到我們的全球聯絡資訊或請致電 02-8722-0711。2017 年 06 月發行。