AKAMAI 產品簡介

API Security

API Security 是一種智慧方法，可保護您的 API 不受業務濫用和資料竊盜

API 是帶動營收的連接組織，也是核心業務流程的推力。它們促成了創新、商業服務和合作夥伴關係。但其中仍然存在著安全性問題。一旦 API 獲得網路應用程式與 API 保護 (WAAP) 產品的授權，資安團隊就無法掌握公司內部對其的運用狀況。惡意攻擊者已察覺此漏洞，轉而開始濫用企業組織內部的廣大 API 攻擊面。

選擇 API Security 的理由

我們的平台讓資安專業人員掌握整個 API 資產的行為可視性。API Security 專為向合作夥伴、供應商和使用者公開其 API 的企業所打造，可為您探查 API、瞭解 API 的風險狀態、分析其行為，並阻止潛藏在內部的威脅。

輕鬆整合，保障隱私

整合過程十分簡單，不需要部署任何針對應用程式的感應器。API Security 並非內嵌模式，它能與您環境中的任何 API 活動資料搭配使用，例如 API 閘道、網路應用程式防火牆、雲端平台、容器或網狀網路環境、反向代理、CDN、資料中心技術，或是登入平台等。

這與我們的 WAAP 產品 Akamai App & API Protector 相輔相成。App & API Protector 是以內嵌模式應對 API 威脅的合適工具，而 API Security 則適用所有方面，以客戶的可預測 API 行為作為基準，監控任何可能出現的異常狀況並傳送警示。

我們支援多種整合選項，可全面探查並保護您的整個 API 資產。API Security 的設計提供隱私保護，在傳輸至 API Security 平台之前，所有資料都會使用憑證化進行匿名。

完整的 API 安全性包括：

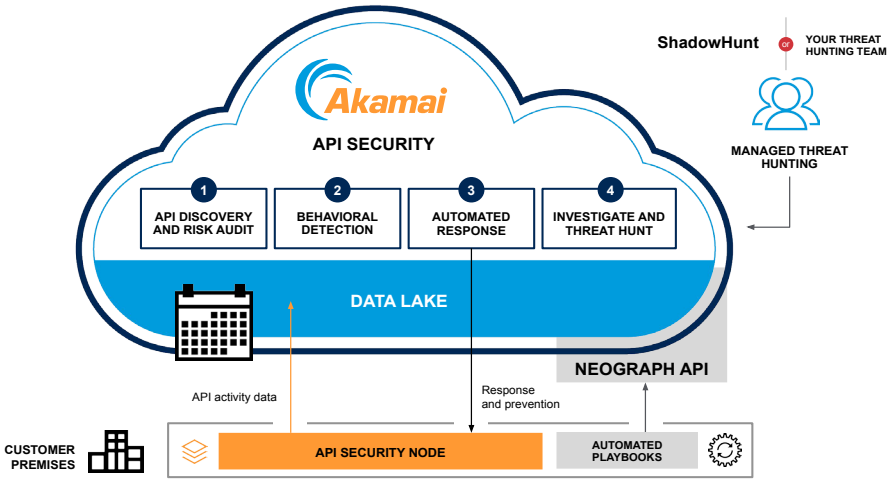
- **App & API Protector**，可探查透過 Akamai Connected Cloud 執行之應用程式與 API，以緩解其 API 威脅，並立即封鎖任何含有潛在威脅的流量，避免讓您的業務受到威脅。
- **API Security**，不受平台限制，可全方位探查企業的所有 API 端點，提供可視性。它能針對 API 活動提供精細的行為分析，並判斷應透過 WAAP 採取的特定回應，以緩解有漏洞或遭入侵的 API 流量。

貴企業可享有的優勢

- 在任何地方都能找到 API
- 取得創新的 API 偵測與回應
- 瞭解警示背後的脈絡
- 利用我們的資料湖泊找出威脅趨勢
- 使用您的資料改善安全性

- **一併部署之後**，Akamai 的解決方案就能全面且持續地提供 API 狀況的可視性，讓您在整個應用程式資產中探查、稽核、偵測和應對 API 安全性疑慮。透過整合 API Security 和 App & API Protector，也能讓您實現最可靠簡單的 API 安全性導入。

在 Gartner® Peer Insights™ 上看看客戶對 API Security 的想法。



> 完善的 API 安全性工具，涵蓋 API 行為和弱點分析。
>
> 旅遊住宿產業的 IT 安全性與風險管理部門經理

需要 API 專家協助您找出威脅？聯絡我們的 API Security ShadowHunt 團隊，他們可以作為您團隊的延伸，調查您的 API 資料。