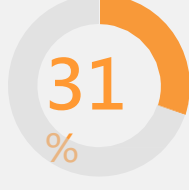


團結就是力量：

Akamai App & API Protector
+ API Security

以API為目標的攻擊不斷增加，這也是全球企業最重視的安全考量。在實行API保護方面，客戶需要分層式的防護方法。搭配使用API Security與Akamai App & API Protector，可阻擋更多的威脅。這些原生連線解決方案可讓您快速部署並自動回應。

API保護需要新的定位



受Akamai保護的
流量為API流量



API點擊次數較
去年同期成長30%



預計2024年
API點擊次數

瞭解API攻擊

Akamai App & API Protector
可防禦這些攻擊

DDoS

攻擊



CVE

惡意探索

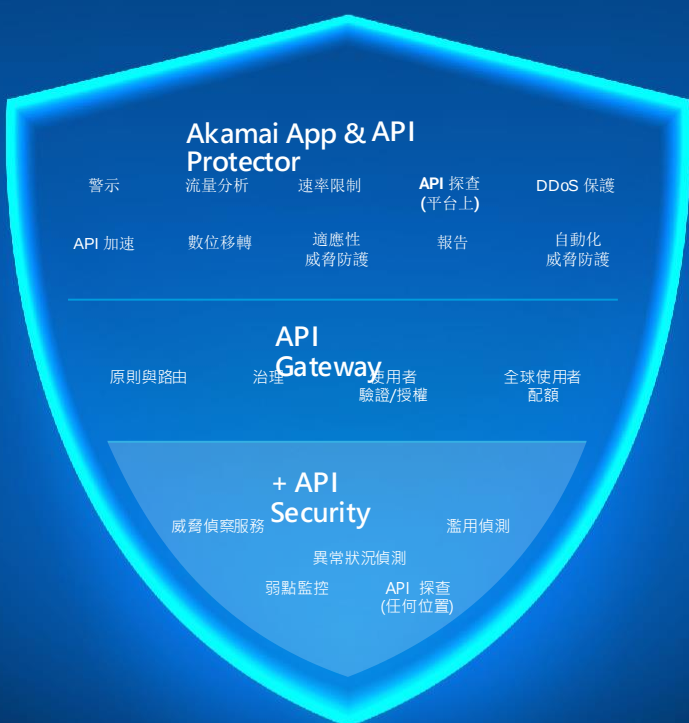
已知的
API攻擊機器人程式
攻擊API Security
可防禦這些攻擊出現破口的
合作夥伴攻擊

邏輯攻擊

外洩的
API

地下API

現今的API攻擊不可同日而語，因此Akamai擴展了解決方案



相輔相成之下，App & API Protector 和API Security

能防禦「OWASP 10 大API」清單所列的安全風險

2023 年API1 - 不良的物件層級授權

2023 年API2 - 不良驗證

2023 年API3 - 不良的物件屬性層級授權

2023 年API4 - 資源消耗量未設限

2023 年API5 - 不良的功能層級授權

2023 年API6 - 機密業務流程存取權未設限

2023 年API7 - 伺服器端偽造要求

2023 年API8 - 安全設定錯誤

2023 年API9 - 不當庫存管理

2023 年API10 - 不安全的API 使用方式

App & API Protector API Security

從導入到因應，為您的企業帶來助益



按一下即可連接

透過原生連接器，您可以連接這兩種解決方案，掌握廣泛的資料可視性



探查各處的API

內嵌和頻外API、未發現的隱藏API、未知API、地下API 和新的API



全球情報

利用Akamai 全球威脅情報，提升您的偵測能力與準確度



規模與效能

防禦巨流量攻擊，同時獲得API 加速和更高的效能



偵測與緩解

即使針對進階攻擊也能獲得深度偵測，並在內嵌環境緩解威脅

若要進一步瞭解，請聯繫 Akamai 專屬諮詢信箱 <ken.lu@netfos.com.tw>。