

最適な組み合わせ：

Akamai App & API Protector
+ API Security

現在、API を標的とした攻撃の増加は、グローバルな組織にとって最大の懸念事項の1つとなっています。お客様の API を保護するためには、レイヤー化された保護アプローチが求められます。API Security と Akamai App & API Protector を組み合わせ、さらに増大する脅威から防御しましょう。これらのソリューションはネイティブに接続されており、迅速に展開でき、自動的に対応します。

API の保護には新たな姿勢が求められる

Akamai が保護した
トラフィックのうち、
API トラフィックの割合API ヒット数が
前年比で 30% 増加2024 年に予測される
API ヒット数

API 攻撃を理解する

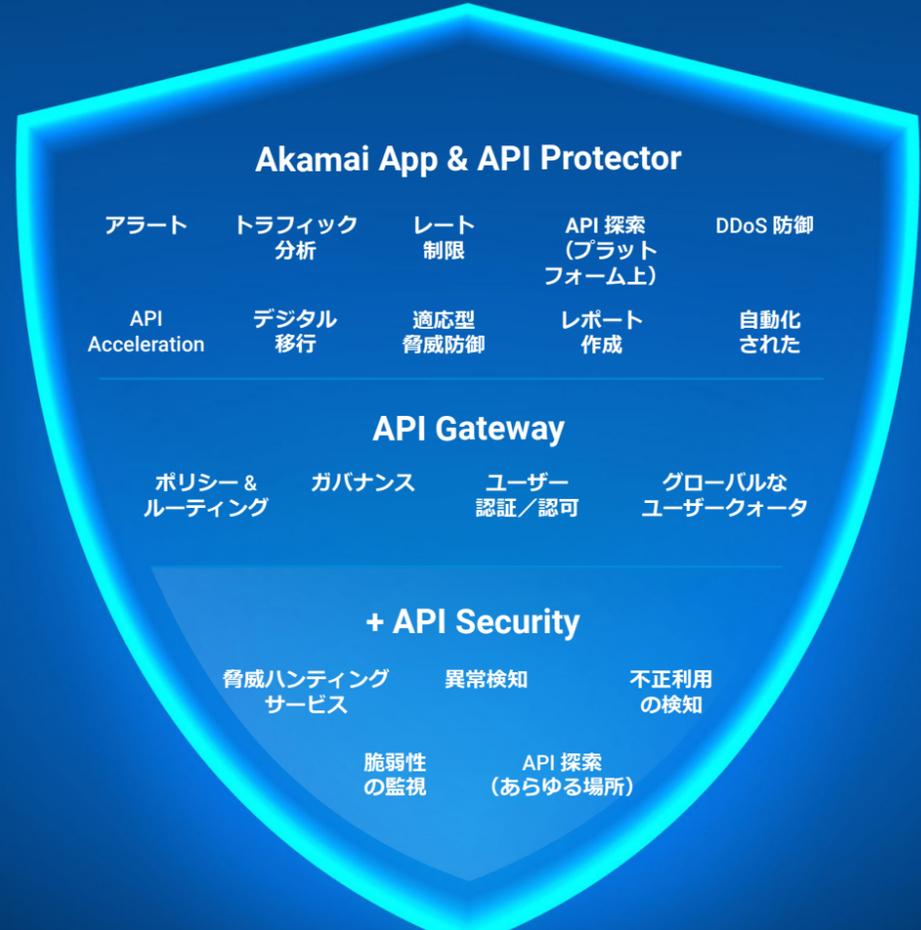
Akamai App & API Protector

以下の攻撃から守ります

DDoS
攻撃CVE
エクスプロイト既知の
API 攻撃ボット
攻撃

API Security

以下の攻撃に対応します

侵害された
パートナー攻撃ロジック
攻撃公開された
APIシャドウ
API従来の攻撃とは異なる新たな API 攻撃に対応するために
拡大してきた Akamai のソリューションApp & API Protector と API Security の組み合わせで
OWASP Top 10 API リストに対応

API1:2023 — オブジェクトレベルの認可の不備 (BOLA)



API2:2023 — 認証の不備 (BA)



API3:2023 — オブジェクトプロパティレベルの認可の不備 (BOPLA)



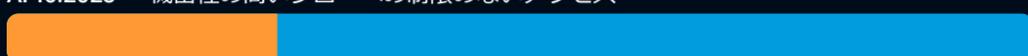
API4:2023 — 制限のないリソース消費



API5:2023 — 機能レベルの認可の不備



API6:2023 — 機密性の高いフローへの制限のないアクセス



API7:2023 — サーバーサイドリクエストフォージェリ (SSRF)



API8:2023 — セキュリティ設定のミス



API9:2023 — 不適切なインベントリ管理



API10:2023 — API の安全でない使用



■ App & API Protector ■ API Security

実装から対応まで、ビジネスにメリットをもたらします

ワンクリックで
接続ネイティブコネクタで両方のソリューションを
接続して、データの可視性を高めることができますどこでも
API を検出インラインおよびアウトオブバンドで、隠れた API、
未知の API、シャドウ API、新規 API を検出しますグローバルイン
テリジェンスAkamai のグローバル脅威インテリジェンスに
アクセスして、検知と精度を向上させますスケーリングと
パフォーマンスボリューム型攻撃から防御しながら、API の高速化
とパフォーマンスの向上を実現します

検知と緩和

高度な攻撃も検知し、インラインで緩和します

詳細については、akamai.com/products/api-security を
ご覧ください。