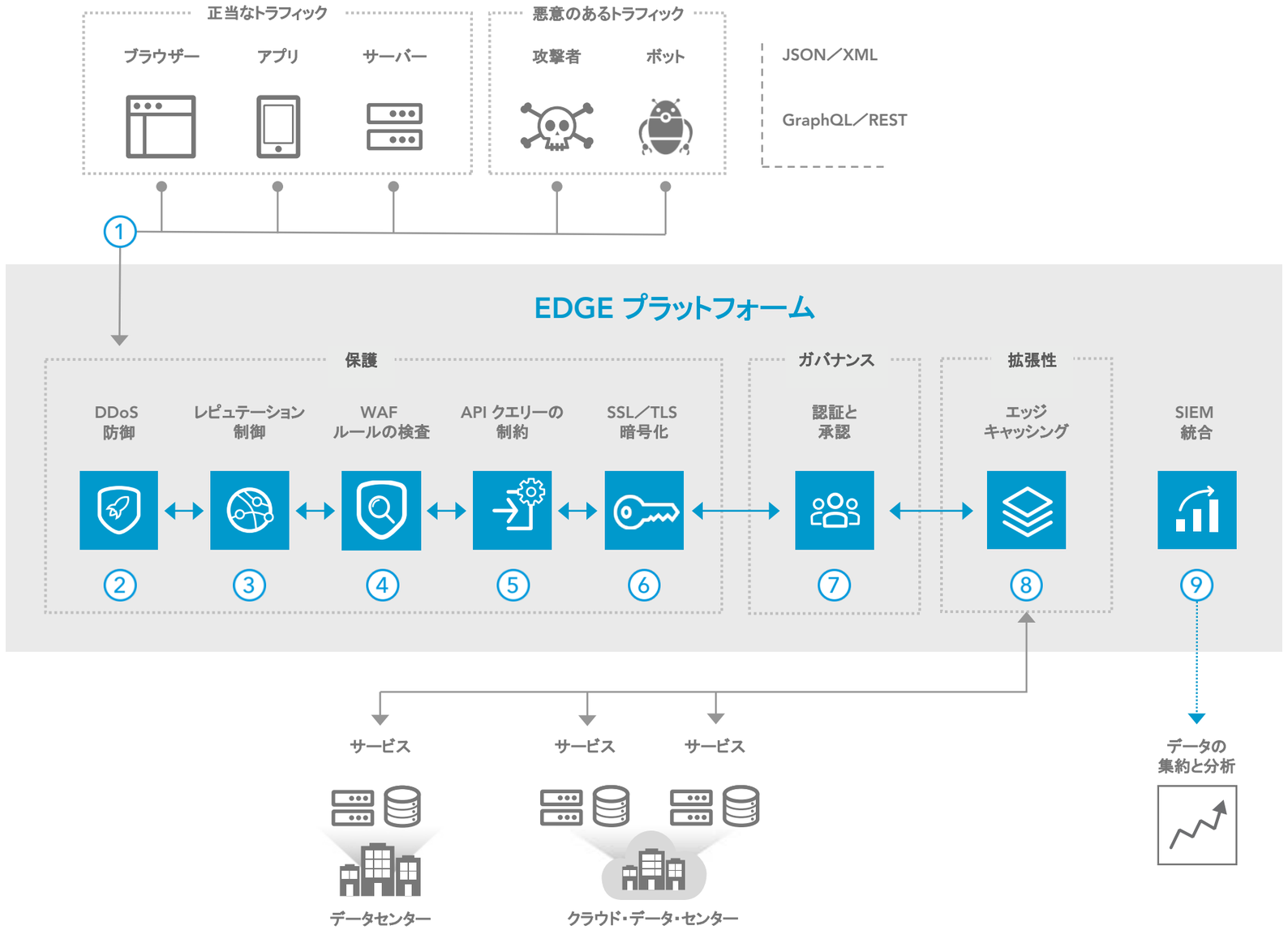
API セキュリティの強化

リファレンスアーキテクチャ



概要

API セキュリティは見過ごされたり、一貫性なく適用されたりすることがよくあります。このような状況では悪意ある攻撃やデータ漏えいに対して脆弱になり、収益やブランド価値が損なわれる可能性があります。Akamai のソリューションはお客様の API を DDoS、アプリケーション攻撃、Credential Stuffing 攻撃から保護します。API の保護は、お客様のインフラストラクチャから遠く離れたエッジで実行されるので、細分化された広範なアタックサーフェス全体でセキュリティ対策が強化されます。

1. 正当なコンシューマーと攻撃者が Akamai Intelligent Edge Platform を通じて API にアクセスします。
2. エッジサーバーがネットワークレイヤーに対する DDoS 攻撃を自動的に破棄し、DDoS やアプリケーション攻撃からアプリケーションレイヤーを守ります。
3. それぞれに固有のレピュテーションスコアに基づき、攻撃者からのトラフィックを阻止します。レピュテーションスコアは、その IP アドレスの以前のふるまいに関する Akamai の可視性によってもたらされます。
4. API リクエストを自動的に検査して悪意のあるコンテンツかどうかを判断し、デバイスのフィンガープリントに基づいて攻撃ツールをブロックします。
5. 個々の API 仕様に基づくポジティブ・セキュリティ・モデルで、データの抽出と挿入を防ぎます。バックエンドのマイクロサービスとアプリケーションを DoS タイプの攻撃から保護します。
6. SSL／TLS 暗号化によって伝送時に機微な情報が露出するのを防ぎます。
7. API ゲートウェイが API リクエストを検証し、正当なコンシューマーが API にアクセスできるようにします。
8. API レスポンスがキャッシュから提供されることで、パフォーマンスが向上し、インフラストラクチャと帯域幅のコストが軽減します。
9. セキュリティ情報とイベントをキャプチャして、保持し、お客様の SIEM アプリケーションにリアルタイムで提供します。

キープロダクト

保護 ▶ Kona Site Defender、Web Application Protector、または Bot Manager
ガバナンス ▶ API Gateway
拡張性 ▶ Ion または Dynamic Site Accelerator
SIEM 統合 ▶ SIEM Connector

公開日：2019 年 8 月