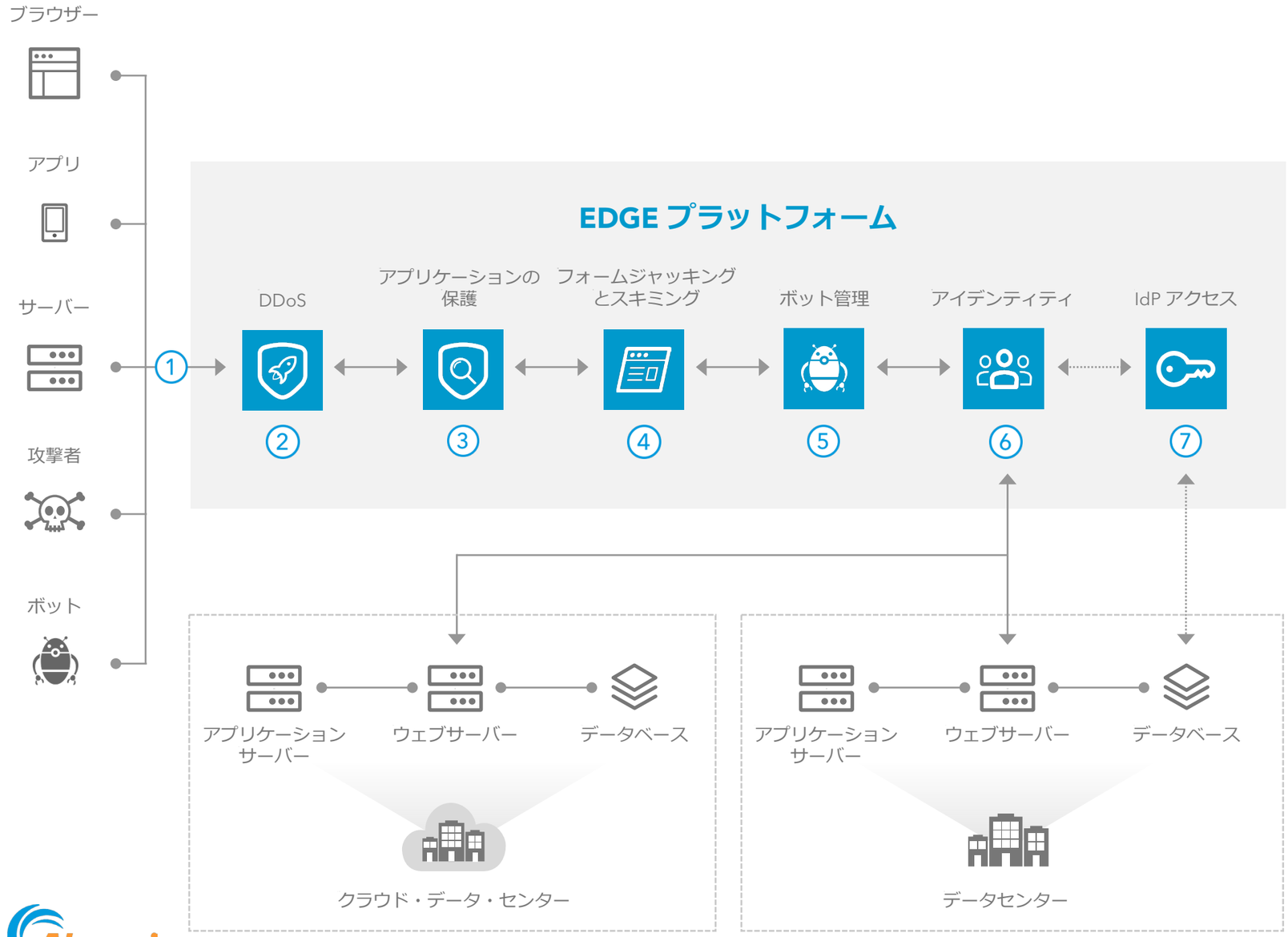
オンライン詐欺とサイバー犯罪の防止

リファレンスアーキテクチャ



概要

金融機関は魅力的なターゲットです。そのため、攻撃ベクトルを常に変化させて検知を回避する巧妙な犯罪者に標的として狙われます。攻撃の成功を許せば、規制違反の制裁が科されるうえ、消費者の信頼を失うというさらに重大な被害も受けることになります。

Akamai のソリューションでは、常に変化する脅威を見越し、その一歩先を行くセキュリティ対策を確立することで、消費者の個人資産を保護できます。また、新たな登録にも簡単に対応できます。

1. Akamai Intelligent Edge Platform は、相互 TLS やその他のネットワーク制御機能、さらに API 認証と許可の主要形式によるアプリケーションアクセスに対応します。
2. DDoS はそれ自体、大きな脅威ですが、攻撃者の本当の目的から標的の注意をそらすために使われることもあります。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、アプリケーションレイヤーへの攻撃を防御します。
3. ウェブリクエストの検査とポジティブ・セキュリティ・モデルによってアプリケーションデータを保護します。これには、API 設定ファイルに定義された特定のパラメーターを使用します。
4. ページのディープインスペクションと分析によって、影響を受けたスクリプトを明らかにし、データを保護します。
5. 最新かつ最も巧妙なボットを特定する機能により、Credential Abuse の試みやアカウント乗っ取り（ATO）の可能性に対抗します。
6. エッジでのカスタマー・アイデンティティ・アクセス管理（CIAM）によって、機微な情報のセキュリティを確保するとともに、パフォーマンス強化、パーソナル化、データ保護、および複雑な規制環境への対応を可能にします。
7. 認証情報をオンプレミスのディレクトリまたはファーストパーティのアプリケーションに保存するオプション。

キープロダクト

DDoS、アプリケーション、フォームジャッキングの防御 ▶ Kona Site Defender

ボット管理 ▶ Bot Manager

アイデンティティおよびアプリケーションアクセス ▶ Identity Cloud および Enterprise Application Access

公開日：2020 年 5 月