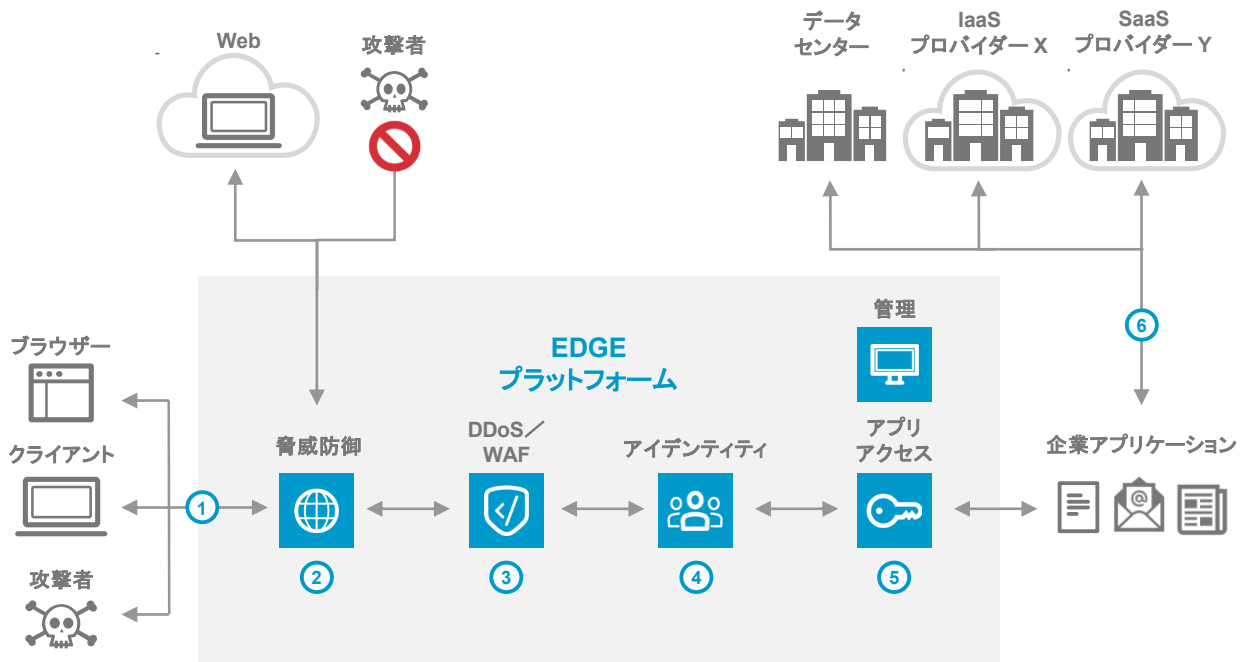


ゼロトラスト・セキュリティ

リファレンスアーキテクチャ



概要

攻撃者は境界から侵入して横方向に移動し、データを盗み出そうとします。ゼロトラスト・セキュリティ・アーキテクチャはそのようなリスクを最小限に抑えます。各ユーザーに最小限の権限のみが付与され、デフォルトではアクセスが拒否されるゼロトラスト・セキュリティ・アーキテクチャでは、一元化されたセキュリティとアクセス制御を通じてユーザーを保護し、アクセスを提供します。ビジネスの要求に応じた、限りあるリソースの拡張にも対応します。

- ① ユーザーが Akamai Intelligent Edge Platform を介して企業アプリケーションや Web にアクセスします。
- ② 脅威防御ソリューションにより、マルウェア、フィッシング、悪意のあるウェブコンテンツなどからユーザーが保護されるとともに、エンタープライズ組織はアクセスの状況を詳細に把握できます。
- ③ エッジサーバーが、企業アプリケーションに対するネットワークレイヤーの DDoS 攻撃を自動的に破棄し、ウェブリクエストを検査して、SQL インジェクション、XSS、RFI などの悪意のある脅威をブロックします。
- ④ ユーザーのアイデンティティは、オンプレミス、クラウドベースのサービス、または Akamai のアイデンティティストアを利用して管理できます。
- ⑤ ユーザーのアイデンティティやその他のセキュリティシグナルに基づき、企業ネットワーク全体ではなく、必要なアプリケーションのみへのアクセス権が付与されます。
- ⑥ Akamai Intelligent Edge Platform が、承認、認証したユーザーを、関連する企業向けアプリケーションにルーティングします。

キープロダクト

脅威防御 ▶ Enterprise Threat Protector
DDoS/WAF ▶ Kona Site Defender または Web Application Protector
アイデンティティ確認とアプリへのアクセス ▶ Enterprise Application Access