

Cequence Platform

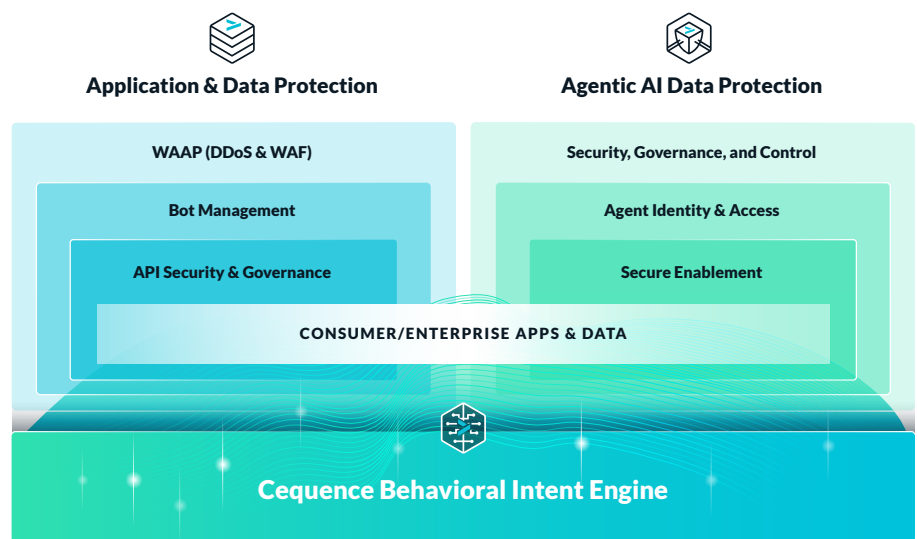
アプリケーション、API、AIのための行動ベース保護

拡大し続ける攻撃対象領域

クラウド活用の拡大、システム間連携の高度化、サードパーティのサプライチェーンへの依存、そしてAIの普及により、企業の攻撃対象領域はかつてない規模で拡大しています。アプリケーションやAPIは増加を続け、AIは攻撃者に脆弱性の発見と機械速度での攻撃を可能にしています。また、適切に統制されていないAIエージェントは、データ漏えいや権限逸脱のリスクをもたらします。企業には、AIがもたらす生産性向上と成長機会を最大限に活用しながら、アプリケーション、API、データを攻撃、ビジネスロジックの悪用、不正行為から保護できるソリューションが求められています。

Cequence独自のアプローチ

あらゆるアプリケーション、API、AIとのインタラクションは、その振る舞いを通じて意図を示します。行動インテント (Behavioral Intent) はCequenceプラットフォームの基盤です。Cequenceは、アプリケーション、API、データとやり取りするすべてのユーザー、ボット、エージェントをプロファイリングし、正当な自動化と悪意ある活動を区別するデジタルアイデンティティを構築します。この機能は現在、エージェント型AIにも拡張されています。Cequenceはエージェントとアプリケーション間のトラフィックに対して行動分析を適用し、エージェントが実行できる操作やアクセス可能なデータをリアルタイムで制御するとともに、許容範囲を超える行動が検出された場合には即座に対処します。



Cequence製品



AI Gateway

エージェント型AIワークフローを接続し保護



Bot Management

アプリケーションとAPIを自動化攻撃や不正行為から保護



API Security

APIエンドポイントの検出、可視化、テスト、保護



WAAP

Bot Management、API Security、WAF、DDoS対策を統合

Cequence AI Gatewayは、組織がアプリケーションやデータをAIエージェントから簡単かつ安全に利用できるようにします。可視化と監視のための一元的な管理基盤に加え、信頼できるMCP、API、LLM、スキルのレジストリ、および企業が承認したアプリケーションカタログを提供します。また、最小権限アクセス、レート制限、機密データ保護などの機能を備えたガバナンスとガードレールを標準搭載し、AIエージェントの振る舞いを適切に制御します。

AI Gatewayには、最小権限アクセス、レート制御、機密データ保護などを含むガバナンス機能とガードレールが組み込まれており、エージェントの行動を適切に制御します。ゼロトラストの原則に基づき、AI Gatewayは実行時に継続的な検証と妥当性確認を実施します。これらのガードレールと制御機能により、企業はガバナンスを維持しながら迅速なイノベーションを実現し、技術的負債やスケーラビリティの制約を抱えることなく、プロトタイプから本番環境への移行を進めることができます。

Cequence API Securityは、APIの検出、インベントリ作成、テストを実行するAIファーストのソリューションであり、包括的なAPIセキュリティポスチャ管理を提供します。内部API、外部API、サードパーティAPIに加え、エッジ、インフラストラクチャ、ゲートウェイ、ホスティングプロバイダーまで幅広く検出します。

内側から外側への検出 (Inside-Out) と外側から内側への検出 (Outside-In) を組み合わせることで、攻撃対象領域と内部APIの両方について可視化とインベントリを実現します。APIセキュリティは、APIを流れる機密データを自律的に特定し、実行時にマスキングすることで、不要なデータ流出を防止します。また、運用担当者を支援するAIアシスタントと、社内のエージェント型AIワークフローと連携するためのMCPサーバーを標準搭載しています。

Cequence Bot Managementは、幅広い自動化攻撃を検出し、データ損失、情報窃取、不正行為を防ぐための緩和ポリシーをリアルタイムで適用します。ネットワークベースで動作するため、既存インフラと容易に統合でき、エージェント、JavaScript、SDKは不要です。

行動フィンガープリントと多次元分析によりビジネスコンテキストを深く理解し、攻撃をリアルタイムでネイティブに検出・ブロックします。ビジネスロジック攻撃、エクスプロイト、自動化ボット活動、オンライン詐欺、OWASP API Security Top 10に含まれる脅威など、幅広いサイバー攻撃に対応します。

Cequence Web Application and API

Protection (WAAP) は、Bot Management、API Security、WAF、DDoS対策を単一のSaaS環境で提供します。共通のトラフィックパイプライン上で統合されたコンポーネントにより、マルチベンダー環境で発生しがちな保護のギャップやルーティングの不整合を解消します。

単一のアプリケーション保護ポータルでWAF、ボット対策、APIセキュリティを一元管理できるため、運用負荷を軽減しながら、すべてのアプリケーションおよびAPIインタラクションに対して一貫した防御を実現します。

主なユースケース



エージェント型AIのセキュリティとガバナンス
可視化、監視、ガードレール、制御



JavaScriptやSDK不要
アプリケーションの改修なしで導入可能



あらゆる環境に導入可能
オンプレミス、SaaS、ハイブリッド環境に対応



ボット攻撃の防止
Web、モバイル、APIアプリケーション全体を保護



ブラックボックスではない
攻撃トラフィック、ポリシー、データへ即時アクセス



安全なエージェント型AI活用
エンタープライズアプリケーションやSaaSを安全にエージェント対応化



オープンアーキテクチャ
データのインポート・エクスポートによりSIEMやWAFとの連携を強化



脆弱性悪用の防止
ゼロデイ攻撃対策とOWASP API Security Top 10、PCI DSSへの対応



APIインベントリとリスク評価
内部・外部・サードパーティAPIを継続的に評価



機密データ漏えい防止
機密データを自動検出・マスキングし流出を防止

Cequenceプラットフォームの特長

行動インテリジェンスと高精度なアイデンティティ

行動インテリジェンスは、ユーザーやエンティティの行動を分析して豊かなデジタルアイデンティティを構築し、組織が悪意のあるボットを招き入れることなく、生産性の高いAIエージェントを安全に活用できるようにします。人間とボットを高精度で識別し、正当な自動化と脅威を正確に区別します。さらに高度な認証が必要な場合には、生体認証チェックにより、CAPTCHAのような不要な摩擦を追加することなく、利用者のデバイスに搭載されたSecure Enclaveを活用できます。

実行時保護とリアルタイム対応

Cequenceは実行時に攻撃を検出し、被害が発生する前に動的に対応します。静的ルールや事後分析に依存するのではなく、ライブトラフィックを継続的に評価し、脅威をリアルタイムで特定して即座に対策を実施します。これにより、正規ユーザーの利用を妨げることなく、アプリケーション、API、データを保護します。

モジュール型アーキテクチャと柔軟な導入

Cequenceは、金融、流通、小売、通信業界をはじめとする世界有数の企業において、1日あたり100億件を超えるアプリケーションおよびAPIインタラクションを分析・保護しています。必要な製品から導入し、要件に応じて拡張することが可能です。SaaS、オンプレミス、ハイブリッド環境への迅速かつ柔軟な導入により、プラットフォームがインフラに適応します。

統合プラットフォームによる一貫した保護

Cequenceプラットフォームは、当初から統合を前提に設計されています。ネイティブ統合により、個別ソリューションを組み合わせる際に生じる死角や運用負荷を排除し、ボット、API、AIの各ユースケースに対して統一された防御を提供します。

「私は脅威アクターとネットワーク境界で対峙したくありません。可能な限りその境界を外側へ押し広げたいのです。Cequenceは、当社の境界の外側で悪意あるトラフィックを遮断できます。この機能によって、当社のセキュリティ態勢は大幅に向上しました。」

Maria Ng
CISO

