CEQUENCE

Cequence API セキュリティ｜データシート

APIセキュリティ・ポスチャ管理／テスト／リメディエーション

なぜ今、APIセキュリティか

いまのビジネスは、APIでつながるアプリケーションの上に成り立っています。APIはネットワークと機密データへの入口であり、攻撃者の最優先ターゲットです。APIの急増により、次のような課題が顕在化しています。

- シャドウ／隠れ／廃止済み／サードパーティAPIの散在
- 機密・個人情報の露出
- 権限昇格を招くコーディングエラー
- ビジネスロジックの悪用

必要なのは、APIを見つけて棚卸しし、仕様や規制への適合性を評価し、ライフサイクル全体（開発～運用）で守るための“API専用”ソリューションです。

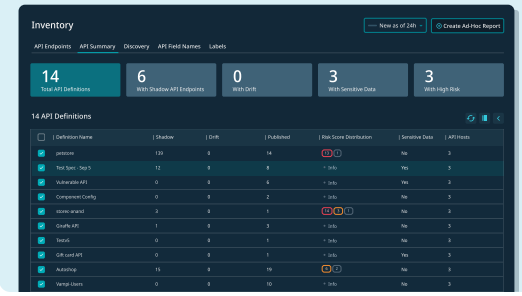
Cequence API セキュリティのポイント

- インフラ連携、インラインセンサー、ドメインスキャンによるAPIの網羅的なディスカバリー（発見）
- 機密データのマスキング、漏えい検知と抑止
- コーディングミスや設定ミスを可視化する継続的なリスク監視
- 開発～本番を通じたAPIセキュリティテストの統合
- データ流出・窃取・不正を防ぐアプリケーション／API保護

ソリューション概要

CequenceはAPIを発見・監視・テストし、コンプライアンスやガバナンスの問題、データ損失や業務停止につながるリスクを幅広く可視化します。内向き／外向き双方のAPIを対象に、変更への追従、機密データの露出把握、OWASP API Security Top 10に代表される脆弱性の特定を支援します。APIセキュリティテストは中核機能で、開発・検証環境と本番環境の双方で仕様に基づく検証を実施。仕様がない場合もOpenAPI仕様を自動生成できます。提供形態はSaaS／オンプレミス／ハイブリッドに対応します
Cequenceが実現すること：

- 仕様がなくても、シャドウ／ゾンビAPIを含む全APIを発見
- 地理情報、ヘッダー、クエリ、ボディ要素などの利用状況を可視化
- 発見したAPIからOpenAPI仕様を自動生成し、準拠を担保
- OWASP API Security／自動化Top 10に基づく動的リスク評価
- 検証環境での合成トラフィックによるテストでリスクを早期に顕在化
- WAFやAPIゲートウェイ等のインフラと連携して防御を自動化



継続的なAPIディスカバリー、インベントリ管理、リスク分類で、APIフットプリントをコントロール。

主な機能

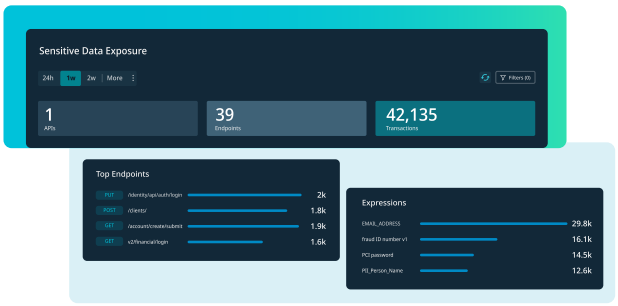
APIフットプリントの継続的な可視化

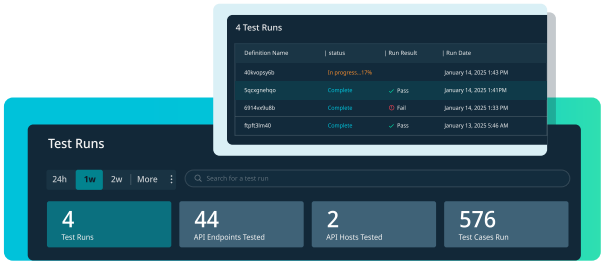
「どのAPIが、どこで、誰に使われているのか？」―多くの企業にとって最大の課題です。Cequenceは、ネットワークレベルの専用センサーと、CDNやAPIゲートウェイなど既存インフラとの連携により、実運用中のAPIフットプリントを継続的に把握します。さらに、ドメイン／サブドメインの外形スキャンで、未使用であっても公開中のAPIホストやエンドポイントを洗い出します。攻撃者の視点でエッジやホスティングも含めて可視化します。

エージェント、JavaScript、SDKの組み込みは不要。非計測のソフトウェアも網羅できるため、開発遅延や表示速度低下、クラウドコスト増を招きません。実行時APIカタログを自動生成し、仕様が無い場合はOpenAPI仕様を自動作成。ダッシュボードでは、リスク別にAPIを一覧し、国・IP・組織別の利用状況までドリルダウンできます。

機密データの漏えい防止

Cequence は、導入後数時間以内に API を自動検出し、ビジネスコンテキストを把握することで、機密情報を取り扱う API を特定します。事前定義およびカスタマイズ可能なデータパターンに加え、自然言語処理（NLP）を活用した機械学習により、文脈を考慮して機密データを検出し、誤検知を低減します。機密データ検出はグローバルに対応しており、国や地域ごとの識別情報を自動的に判別可能です。結果はダッシュボード上で視覚的に表示され、漏えい元の API、レスポンスコード、IP アドレスなどの詳細を確認できます。Slack や PagerDuty、メールによる通知により迅速な是正対応を支援し、さらにフォーマット保持暗号（FPE）によるデータマスキングで、機密情報のプライバシーを確実に保護します。



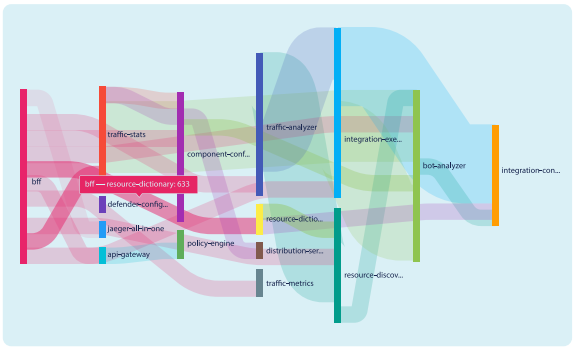


インテリジェントAPIセキュリティテスト

開発・運用の両段階でAPIを徹底検証し、コーディングエラー、脆弱性、仕様逸脱を検出します。仕様が無い場合は自律生成でAPI仕様を作成し、手作業を大幅に削減。CI/CDパイプラインやIDEに組み込めるほか、本番環境で単体実行も可能です。

APIトラフィックフローの可視化

Cequence Flow GraphでAPI間の呼び出し関係を一目で把握。社内APIとサードパーティAPI、その依存関係を特定し、許可済みの連携を検証します。異常やポスチャの抜け漏れを発見し、シャドウ／不正APIを洗い出します。

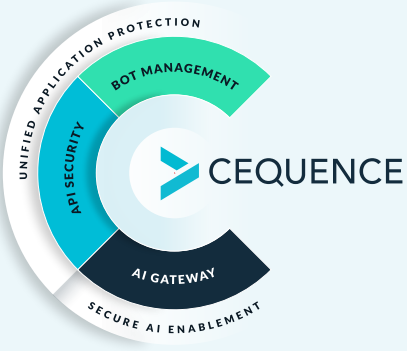


脅威からの保護

ウェブ／モバイル／APIアプリケーションを保護し、データ流出や不正を防止します。MLベースの脅威検知・分析と、WAF／APIゲートウェイ等との連携により、高度な攻撃にも対応します。Cequence Bot Managementは、ブロック、レート制限、ヘッダー挿入、デセプションなどのネイティブ対策を提供します。

API Securityは、Cequence Unified Application Protection（UAP）プラットフォームの一部です

Cequence Unified Application Protection（UAP）プラットフォームは、ディスカバリー／コンプライアンス／プロテクションを統合し、組織のアプリケーションとAPIを攻撃・ビジネスロジックの悪用・不正から守ります。価値を数分で実証（従来の数日～数週間ではなく）でき、アプリの計測や改修を必要としない柔軟なデプロイモデルを提供します。最大規模で要求水準の高い民間・公共機関から信頼され、Cequenceは1日100億件超のAPIインタラクションと40億のユーザーアカウントを保護しています。



CEQUENCE
5201 Great America Pkwy, Suite 240, Santa Clara, CA 95054 | 1-650-437-6338 | info@cequence.ai | www.cequence.ai