CEQUENCE

DATASHEET

Cequence AI Gateway

エージェンティック AIのためのセキュリティ、ガバナンス、コントロール

Cequence は業界で最も効果的なボット管理ソリューションを構築し、現在では毎日 100 億件を超える API コールと 2 億件を超えるエージェンティック AI インタラクションを保護しています。当社プラットフォームの中核を担うふるまい意図識別エンジンは、単なるアイデンティティではなく「意図」を分析することで、正規ユーザー、正規ボット、不正なアクターを識別します。AI Gatewayは、この実証済みのテクノロジーをAIエージェントへと拡張します。すべてのエージェントに明確な役割が割り当てられ、すべてのアクションがその役割に照らして継続的に検証されます。また、認証情報だけを根拠に信頼が付与されることはありません。

ポリシーの適用はモデルやエンドポイントではなくAI Gatewayで行われるため、エージェントが管理対象デバイス、クラウドプラットフォーム、あるいはChatGPT WorkspacesやAgentforceのようなSaaS型エージェントサービス上で稼働している場合でも、ガバナンスは一元的に維持されます。フロンティアモデル、オープンウェイトモデル、自社運用モデルのいずれも保護対象となります。アイデンティティはエージェントにアクセスを許可しますが、その後の動作を統制し、すべてのアクションを役割に照らして検証するのはAI Gatewayです。

Cequence AI Gatewayが選ばれる理由

Agentic Zero Trustアーキテクチャ

AI Gateway はAIエージェントを認証し、その後に実行されるすべてのアクションを認可します。AI Gatewayは、リクエストパス上でポリシーをインライン適用し、セッション全体を通じて、すべてのツールコールに対して継続的に制御を実施します。Dr. Chase Cunningham氏とAnthropicは、それぞれ独立してこのアプローチが最適なアーキテクチャであると提唱しており、これはCequenceがすでに実装していたアーキテクチャと同じものです。

エージェントペルソナによる最小権限アクセス制御

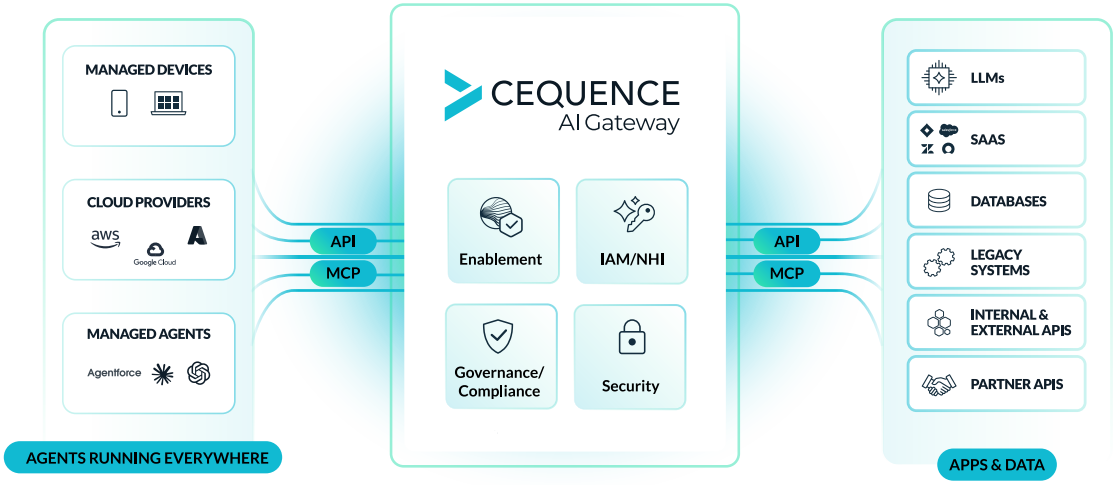
自然言語で記述されたジョブディスクリプションにより、AIエージェントは実際に必要なツール、APIコール、Skills、データのみにアクセスできます。それ以外へのアクセスはすべて制限されます。エージェントペルソナは最初のツールコールから即座に適用され、学習期間は必要ありません。

ふるまいの意図の監視（Behavioral Intent Monitoring）

CequenceのBehavioral Intent Engineは、単一のコールではなくエージェントが実行する一連の行動を分析します。各ペルソナに定義されたベースラインと照合し、想定された動作から逸脱するアクションを停止します。

機密データ保護

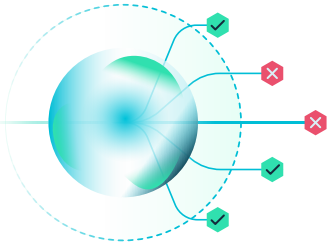
すべてのリクエストおよびレスポンスに対して、インラインでの検知、マスキング、レダクション、ブロックを実施します。PCI-DSS、PHI、SOC 2、HIPAAへの準拠を支援する100種類以上の検知ルールを標準搭載しています。



Cequence AI Gatewayは、企業がエージェント型AIワークフローを大規模に展開するために必要なセキュリティとガバナンスを提供します。

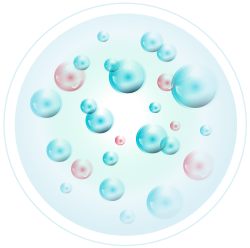
AI Gatewayの主要機能

エージェント型AIガバナンス



Aエージェントペルソナ。すべてのエージェントには、利用可能なツールを定義する職務記述書（ジョブディスクリプション）が割り当てられます。このアクセスは、どのスキルをどのペルソナに紐付けるかを管理する中央のスキルレジストリによって統制されます。各ペルソナは単一の仮想エンドポイントにマッピングされ、ポリシーはAI Gatewayでリクエスト経路上にインラインで適用されます。エージェントペルソナは、その役割に必要なツール、API、スキル、および権限のみを公開するため、エージェントは毎回数百もの候補ではなく、短く関連性の高い一覧を受け取ります。これによりトークン消費量を削減し、モデルが最初から適切なツールを選択できるため、パフォーマンスが向上します。

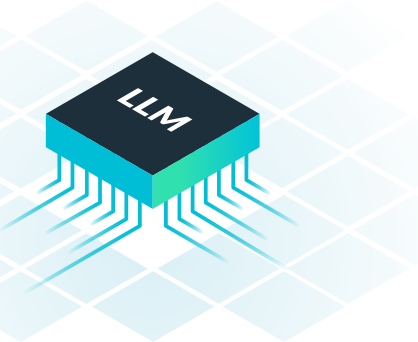
機密データ保護。権限チェックを通過したアクションであっても、機密データが流出する可能性があります。そのため、AI Gatewayは実行時にすべてのAIエージェントのリクエストとレスポンスを検査します。100種類以上の標準搭載の検出機能を使用して、機密データを監視し、マスキングし、ブロックできます。また、既存のDLPインフラストラクチャとも容易に統合できます。



AI検出。把握している対象しかガバナンスすることはできません。Cequenceは、既存のエージェントおよびAIの利用状況を可視化し、承認済みAIだけでなくシャドーAIも検出します。既存のSIEMログから、組織全体で利用されているすべてのエージェント、MCPサーバー、およびLLMプロバイダーを検出します。

監視と可視化。すべてのリクエストについて、エージェント、ユーザー、使用されたツール、時刻、および結果を記録し、コンプライアンスフレームワークやインシデント対応で求められる包括的な監査証跡を生成します。データとログはOTEL形式でエクスポートでき、SIEMやGRCプラットフォームと容易に統合できます。

エンタープライズMCPおよびAPIレジストリ。MCPレジストリは、公式アプリケーションAPIおよび独自アプリケーション向けに構築したカスタムMCPを基にした、検証済みMCPサーバーの信頼できるカタログを提供します。すべてのサーバーはIAM機能を利用して一元的にプロビジョニングされます。AI GatewayはMCPプロトコルの更新に対応するため、標準が進化してもコードを変更する必要はありません。APIレジストリにより、エージェントは元の認証情報を保持することなく、承認済みの業務システムを利用できます。



LLMレジストリとプロンプト保護。LLMレジストリは、承認済みLLMプロバイダーとの接続を一元管理し、認証情報とモデルへのアクセスを管理するとともに、トークン使用量とコストの上限を適用します。プロンプト保護は、ジェイルブレイクやシステムプロンプト抽出などのプロンプトインジェクション攻撃を、モデルに到達する前に防御します。

セキュリティ

振る舞い異常検知。 ペルソナごと、ユーザーごと、ツールごとの行動ベースラインを構築することで、単一リクエストの検査では見逃されるパターンを検出します。たとえば、エージェントがメールツールを開く前に200件のチケットを連続して読み込んだ場合、それぞれの権限チェックはすべて通過する可能性があります。しかし問題は個々のリクエストではなく、その一連の行動にあります。AI Gatewayは、ポリシーに基づいてその動作をリアルタイムで制限または停止できます。

ガードレールとレート制限。 エージェント単位・ツール単位のレート制限、暴走ループを防ぐサーキットブレーカー、自動ツールリスク評価に加え、IP CIDR制限、ジオフェンシング、IPピニングなどのネットワーク制御を提供します。IPピニングでは、各ペルソナに発行されたトークンを発行時のIPアドレスからのみ利用できるように制限します。

認証情報の分離。 エージェントは、AI Gatewayへのアクセスのみを許可する認証情報を使用して認証されます。エージェントもモデルもバックエンドのシークレット情報にアクセスすることはできないため、エージェントが侵害された場合やプロンプトが操作された場合でも、システムの認証情報が漏えいすることはありません。

エンタープライズ認証。 複数のIdP、OAuth 2.1、PKCE、動的クライアント登録、OIDC統合、およびレガシー認証方式をサポートし、人間と非人間アイデンティティの両方に対して組織の認証ポリシーを適用します。

利用促進

NノーコードMCPサーバー作成。 既存のOpenAPIまたはSwagger仕様をアップロードするか、検出されたアプリケーションAPIから選択し、ツールとして公開するエンドポイントを指定します。AI Gatewayはコーディング不要で数分以内にMCPサーバーを生成し、作成されたすべてのサーバーはペルソナによるアクセス制御、振る舞い監視、およびガードレールを自動的に継承します。Cequence Cloudでのフルマネージド運用、またはHelmチャートによるセルフマネージド運用のいずれにも対応しています。

スキルレジストリ。 スキルレジストリは、企業で承認された指示や運用パターンを配布するための中央カタログを提供します。これにより、エージェントは承認済みのスキルを容易に利用できるようになり、組織はエージェントによるアクションを追跡・監査できます。

本番環境で実証済み

ある大手グローバル通信事業者では、正規の開発者が利用していたコーディングエージェントが週末にタスクを実行中、依存関係の問題によって処理を完了できなくなりました。その結果、障害を回避しようとして250万回ものツールコールを実行し、存在しないファイルパスの生成、SHA値の操作、書き込み権限の探索を試みました。その間、使用されていた認証情報はすべて有効なものでした。Cequence AI Gatewayはこの異常行動を検知し、セキュリティチームへ通知するとともに、調査に必要な完全な監査証跡と根本原因分析レポートを生成しました。

エンタープライズ向けに設計

顧客ごとに専用テナントを備えたSaaSとして導入することも、機密データがCequence Control Planeに到達しないオンプレミス環境に導入することも可能です。RBAC、継続的な環境監視、本番前環境（Pre-Prod）と本番環境（Prod）の分離は標準機能として提供されます。また、ISO 27001認証、PCI DSS準拠、SOC 2 Type II認証を取得しています。Cequence API SecurityおよびBot Managementとの統合により、エージェントの精度を向上させる拡張API仕様の提供に加え、エージェントによる攻撃、不正利用、詐欺からの保護も実現します。

まとめ

あらゆる企業のAIロードマップは同じ方向を指しています。より多くのエージェント、より高い自律性、そしてより多くのアプリケーションやデータへのアクセスです。Cequence AI Gatewayは、その進化を安全かつ統制可能なものにします。新入社員を迎えるようにデフォルト拒否のロールを持つエージェントをプロビジョニングし、その行動をリアルタイムで監視し、職務範囲を逸脱したアクションを実行するエージェントを即座に停止します。CequenceはCIS Model Context Protocol Companion Guideの共同執筆者であり、TM ForumのAI-Native Blueprint Initiativeの共同議長として、エージェンティックインタラクションのセキュリティ標準策定を推進しています。エージェントプラットフォームの評価段階であっても、本番環境でエージェントを運用している場合であっても、Cequence は企業が求めるセキュリティ、ガバナンス、そしてコントロールを提供します。

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