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 Behavioral Intent Engine 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。Frontier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はエージェントを認証した後、そのすべてのアクションを個別に認可します。Gatewayはリクエスト経路上でインラインにポリシーを適用し、セッション全体および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氏およびAnthropicによる独立した研究は、Cequenceがすでに構築していたものと同じアーキテクチャへと到達しています。

Agent Personasによる最小権限アクセス制御

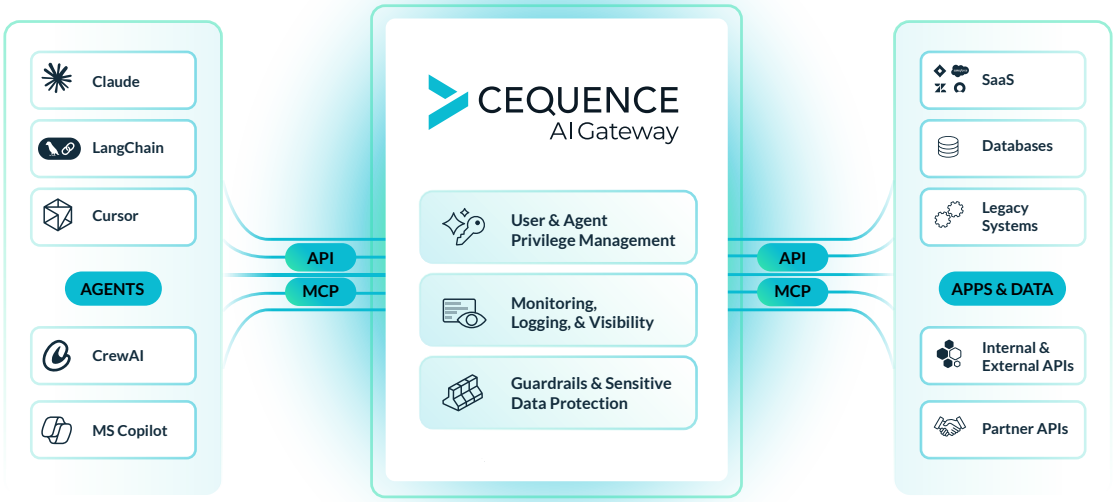
自然言語による職務記述は、デフォルト拒否（Default Deny）のロールへ変換され、特定のMCPツール、API操作、データオブジェクトに対するツールコール単位の権限のみが付与されます。Personaは学習期間を必要とせず、最初のツールコールから即座に適用されます。

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Persona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。

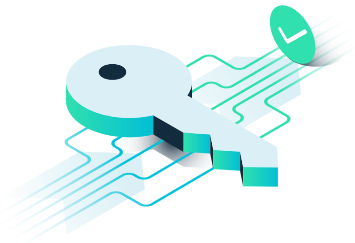


Cequence AI Gatewayは、企業がエージェント型AIワークフローを大規模に展開するために必要なセキュリティとガバナンスを提供します。

AI Gatewayの主要機能

エージェントのアイデンティティおよびアクセス管理

Agent Personas。 すべてのエージェントには職務記述が割り当てられ、その内容に基づいて利用可能なツールが決定されます。この管理は、どのスキルをどのPersonaに紐付けるかを定義する中央集約型のSkill Registryによって行われます。各Persona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上でインラインに適用されます。Agent Personasは、その役割に必要なツールのみを公開するため、エージェントは毎回数百のツールを受け取る代わりに、必要最小限のツールリストのみを受け取ります。これによりトークン消費を削減するとともに、モデルが最初から適切なツールを選択できるため、パフォーマンスも向上します。



Credential Isolation。 エージェントはGatewayへのアクセスのみを許可する認証情報を用いて認証されます。エージェントやモデルがバックエンドのシークレット情報を参照することはないため、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 。

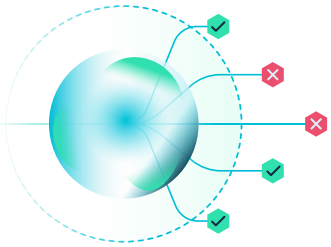
エンタープライズ認証。 OAuth 2.1、PKCE、動的登録（Dynamic Registration）、OIDC統合、およびレガシー認証方式をサポートし、人および非人間アイデンティティの双方に対して組織の認証・認可ポリシーへの準拠を実現します。

ガバナンスとコンプライアンス

モニタリングと可視化。 すべてのリクエストについて、エージェント、ユーザー、ツール、時刻、結果が記録されます。これにより、コンプライアンス要件やインシデント対応で求められる改ざん不可能な監査証跡（Audit Trail）が生成されます。データおよびログはOTEL形式でエクスポートでき、SIEMやGRCプラットフォームとの統合が可能です。

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、機密データの流出につながる可能性があります。そのためGatewayは、転送中のすべてのリクエストとレスポンスを検査します。許可されたツール間での機密データ移動をブロックし、Personaごとのベースラインに基づいて不自然なデータ収集を検知し、ツール引数内の認証情報をマスキングします。また、本番環境データが開発環境や外部ツールへ送信されることを防止します。既存のDLP基盤との統合も容易です。

セキュリティ



行動異常検知。 Personaごと、ユーザーごと、ツールごとに定義された行動ベースラインにより、単一コールの検査では検出できないパターンを発見します。例えば、ある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で読み取った場合、それぞれのアクションは個別には許可されるかもしれません。しかし問題はその行動シーケンスにあります。Gateway はポリシーに基づき、その活動をスロットリングできます。

Guardrailsとレート制御。 エージェント単位およびツール単位のレート制限、暴走ループを防ぐCircuit Breaker、自動ツールリスク評価を提供します。また、IP CIDR制限、ジオフェンシング、トークンを発行されたIPアドレスからのみ利用可能にするIP Pinningなどのネットワーク制御機能もPersona単位で適用できます。

導入支援

ノーコードによる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するだけで済みます。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、生成されたすべてのサーバーにはPersonaによるスコープ制御、行動監視、ガードレールが自動的に適用されます。Cequence Cloudでのフルマネージド運用、またはHelm Chartによるセルフマネージド運用のいずれにも対応します。

エンタープライズMCPレジストリ。 公式アプリケーションAPIから構築された検証済みサーバーのカタログと、自社アプリケーション向けのカスタムMCPにより、シャドーMCPや不正 MCP サーバーを排除します。すべての MCPはIAM機能とともに一元管理されます。また、GatewayがMCPプロトコルの更新に対応するため、標準の進化に伴うコード変更は不要です。

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