

Cequence AI Gateway

Sécurité, gouvernance et contrôle pour l'IA agentique

Cequence a développé la solution de gestion des bots la plus performante du marché et sécurise aujourd'hui plus de 10 milliards d'appels API et 200 millions d'interactions agentiques chaque jour. Le moteur d'analyse de l'intention comportementale au cœur de notre plateforme distingue les utilisateurs légitimes, les bots autorisés et les acteurs malveillants en analysant leur intention, et non uniquement leur identité. AI Gateway étend cette technologie éprouvée aux agents IA : chaque agent se voit attribuer une mission définie, chaque action est continuellement vérifiée par rapport à cette mission, et la confiance n'est jamais accordée sur la seule base d'un identifiant ou d'une authentification.

Parce que l'application des politiques de sécurité s'effectue au niveau de l'AI Gateway plutôt qu'au sein du modèle ou du point de terminaison, la gouvernance reste centralisée quel que soit l'environnement d'exécution des agents : postes de travail gérés, plateformes cloud ou services SaaS d'agents tels que ChatGPT Workspaces et Agentforce. Les modèles frontier, open-weight et auto-hébergés sont tous protégés. L'identité permet à l'agent d'accéder aux ressources ; l'AI Gateway gouverne ce qu'il peut faire ensuite et vérifie chacune de ses actions au regard de son rôle.

Ce qui distingue Cequence AI Gateway



Architecture Agentic Zero Trust

AI Gateway authentifie les agents, puis autorise chacune des actions qu'ils entreprennent. La passerelle applique les politiques de sécurité directement dans le chemin de la requête, pendant toute la durée de la session et à chaque appel d'outil. Le Dr Chase Cunningham et Anthropic ont décrit indépendamment cette approche comme la bonne architecture ; c'est le même modèle que Cequence avait déjà mis en œuvre.



Accès à privilège minimal avec Agent Personas

Une description du poste formulée en langage clair garantit que les agents n'accèdent qu'aux outils, appels d'API, LLM, compétences et données spécifiques dont ils ont réellement besoin — tout le reste demeure inaccessible. Les personas sont opérationnels dès le premier appel d'outil, sans aucune période d'apprentissage.



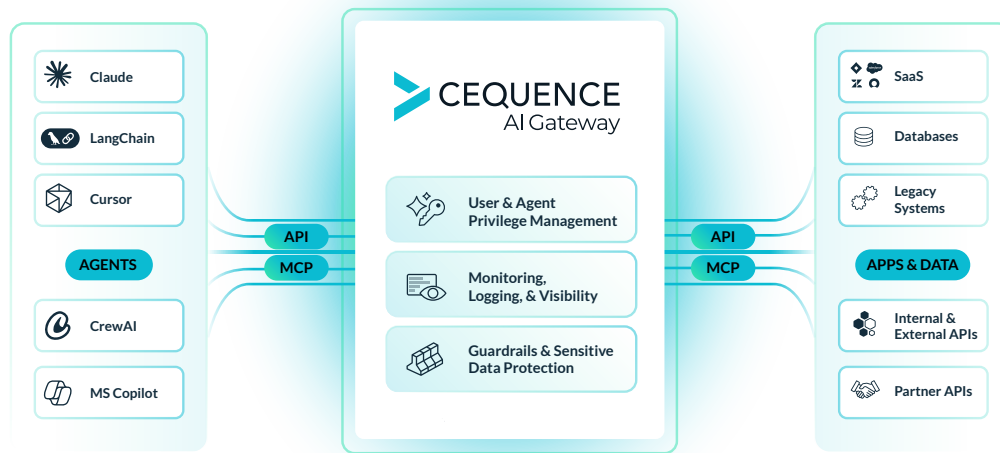
Surveillance de l'intention comportementale

Le moteur d'analyse comportementale de Cequence évalue la séquence d'actions réalisée par un agent, et non chaque appel pris isolément, en la comparant à des références comportementales propres à chaque Persona. Les actions qui s'écartent de ces références sont immédiatement interrompues.



Protection des données sensibles

Détection, masquage, anonymisation et blocage en ligne sur chaque requête et chaque réponse, avec plus de 100 types de détection intégrés prenant en charge les exigences de conformité PCI-DSS, PHI, SOC 2 et HIPAA.

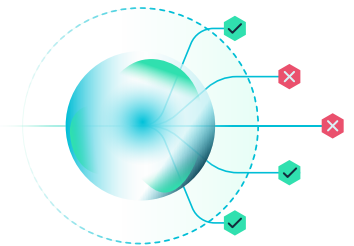


Cequence AI Gateway fournit la sécurité et la gouvernance dont les entreprises ont besoin pour déployer en toute confiance des workflows d'IA agentique à grande échelle.

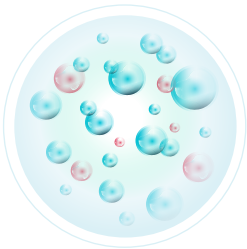
Fonctionnalités d'AI Gateway

Gestion des identités et des accès des agents

Personas d'agents. Chaque agent reçoit une description de poste qui détermine son accès aux outils. Cet accès est régi par un registre centralisé des compétences, qui définit quelles compétences sont associées à chaque persona. Chaque persona correspond à un seul endpoint virtuel, et les règles sont appliquées en temps réel au niveau de l'AI Gateway. Les personas d'agents n'exposent que les outils, API, LLM, compétences et autorisations nécessaires à la fonction. L'agent reçoit ainsi une liste courte et pertinente plutôt que des centaines d'options à chaque requête, ce qui réduit la consommation de jetons et améliore les performances en permettant au modèle de sélectionner le bon outil dès la première tentative.



Protection des données sensibles. Certaines actions peuvent passer les contrôles d'autorisation tout en exfiltrant des données sensibles. C'est pourquoi l'AI Gateway inspecte chaque requête et chaque réponse des agents d'IA pendant leur exécution. Surveillez, masquez et bloquez les données sensibles grâce à plus de 100 types de détection prêts à l'emploi. La solution s'intègre facilement à l'infrastructure DLP existante.

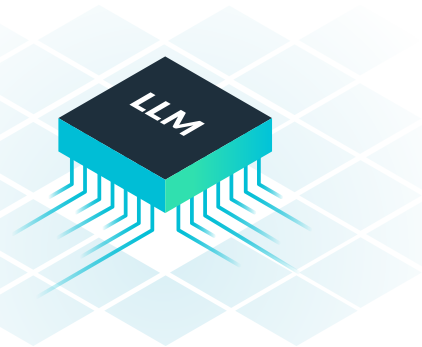


Découverte de l'IA. Vous ne pouvez gouverner que ce dont vous avez connaissance. Cequence offre une visibilité sur l'utilisation actuelle des agents et de l'IA, qu'elle soit autorisée ou non encadrée (« shadow AI »). À partir des journaux SIEM existants, la solution identifie à l'échelle de l'entreprise chaque agent, serveur MCP et fournisseur de LLM.

Surveillance et visibilité. Chaque requête consigne l'agent, l'utilisateur, l'outil, l'heure et le résultat, créant ainsi la piste d'audit complète exigée par les référentiels de conformité et les procédures de réponse aux incidents. Les données et les journaux peuvent être exportés au format OTEL afin de faciliter leur intégration aux solutions SIEM et GRC.

Registres MCP et API d'entreprise. Le registre MCP fournit un catalogue fiable de serveurs MCP validés, créés à partir des API officielles des applications, ainsi que de MCP personnalisés destinés à vos propres applications. L'ensemble est provisionné de manière centralisée et intègre des fonctionnalités IAM. L'AI Gateway prend en charge les évolutions du protocole MCP, de sorte qu'aucune modification du code n'est nécessaire à mesure que la norme évolue. Le registre des API permet aux agents d'appeler des systèmes métier approuvés sans détenir les identifiants d'accès aux systèmes d'origine.

Registre des LLM et Prompt Guard. Le registre des LLM fournit une connexion contrôlée à chaque fournisseur de LLM approuvé, gère les identifiants et l'accès aux modèles, et applique des limites de débit de jetons et de dépenses. Prompt Guard protège contre les injections de prompts, notamment les techniques de contournement des restrictions (« jailbreak ») et les tentatives d'extraction du prompt système, avant qu'elles n'atteignent le modèle.



Sécurité

Détection des anomalies comportementales. Des profils comportementaux de référence établis par persona, par utilisateur et par outil permettent de détecter les schémas qui échappent à l'inspection d'un appel isolé. Un agent qui consulterait 200 tickets d'affilée avant d'ouvrir un outil de messagerie réussirait chaque contrôle d'autorisation individuel. Dans ce cas, c'est la séquence elle-même qui constitue l'infraction, et l'AI Gateway ralentit ou interrompt l'opération en cours selon la politique définie.

Garde-fous et limites de débit. Des limites de débit par agent et par outil, accompagnées de coupe-circuits pour arrêter les boucles incontrôlées, d'une évaluation automatisée des risques liés aux outils et de contrôles réseau comprenant des restrictions par plages IP CIDR, le géopérage et l'épinglage d'adresse IP. Ce dernier impose, pour chaque persona, que les jetons soient utilisés depuis l'adresse IP à laquelle ils ont été délivrés.



Isolation des identifiants. L'agent s'authentifie auprès de l'AI Gateway à l'aide d'un identifiant qui lui donne uniquement accès à la passerelle. Ni l'agent ni le modèle n'ont accès aux secrets des systèmes back-end. Ainsi, un agent compromis ou un prompt manipulé ne peut pas divulguer les identifiants d'accès à vos systèmes.

Authentification d'entreprise. La prise en charge de plusieurs fournisseurs d'identité, avec OAuth 2.1, PKCE, l'enregistrement dynamique, l'intégration OIDC et la compatibilité avec les mécanismes d'authentification existants, permet d'appliquer la politique d'identité de l'organisation aux identités humaines comme non humaines.

Mise en œuvre

Création de serveurs MCP sans code. Importez une spécification OpenAPI ou Swagger existante, ou choisissez parmi les API d'applications découvertes, puis sélectionnez les endpoints à exposer comme outils. L'AI Gateway génère en quelques minutes un serveur MCP sans aucune programmation. Chaque serveur ainsi créé bénéficie automatiquement de la définition du périmètre par persona, de la surveillance comportementale et des garde-fous. Déployez-le en mode entièrement géré dans Cequence Cloud ou en mode autogéré à l'aide d'un chart Helm.



Registre des compétences. Le registre des compétences fournit un catalogue centralisé permettant de diffuser les instructions et les modes opératoires approuvés par l'entreprise. Il facilite l'utilisation des compétences approuvées par les agents et permet à l'organisation de suivre et d'auditer les actions agentiques.

Éprouvé en production

Un grand opérateur mondial de télécommunications a découvert que l'agent de programmation d'un développeur autorisé avait exécuté une tâche pendant le week-end. Après avoir rencontré des dépendances qui l'empêchaient de terminer son travail, l'agent a tenté d'effectuer 2,5 millions d'appels d'outils pour contourner l'obstacle : création de chemins de fichiers fictifs, manipulation des empreintes SHA de fichiers et recherche d'accès en écriture. Tous les identifiants sont restés valides pendant toute la durée de l'incident. Cequence AI Gateway a détecté le comportement anormal, alerté les équipes de sécurité et généré une piste d'audit complète ainsi qu'un rapport d'analyse des causes profondes pour les besoins de l'enquête.

Conçu pour l'entreprise

Déployez la solution en mode SaaS complet, avec un tenant dédié à chaque client, ou sur site afin que vos données sensibles n'atteignent jamais le plan de contrôle de Cequence. Le contrôle d'accès basé sur les rôles (RBAC), la surveillance continue de l'environnement et les modes distincts de préproduction et de production sont proposés en standard. La plateforme est certifiée ISO 27001, conforme à la norme PCI DSS et dispose d'un rapport d'attestation SOC 2 de type II. L'intégration avec Cequence API Security et Bot Management fournit des spécifications d'API enrichies qui améliorent la précision des agents, ainsi qu'une protection contre les attaques, les abus et la fraude alimentés par des agents.

Résumé

Toutes les feuilles de route de l'IA en entreprise suivent la même direction : davantage d'agents, une autonomie accrue et un accès élargi aux applications et aux données. Cequence AI Gateway permet de maîtriser cette évolution : provisionnez chaque agent comme une nouvelle recrue, avec un rôle appliquant le principe de refus par défaut, surveillez son comportement en temps réel par rapport à ce rôle et arrêtez les agents dont les actions s'écartent de leur description de poste. Cequence a coécrit le CIS Model Context Protocol Companion Guide et copréside la AI-Native Blueprint Initiative du TM Forum, contribuant ainsi à définir les normes de sécurisation des interactions agentiques. Que vous soyez en train d'évaluer des plateformes d'agents ou que vous exploitiez déjà des agents en production, Cequence fournit la sécurité, la gouvernance et le contrôle dont les organisations ont besoin.