CEQUENCE

DATASHEET

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 de leurs actions. Le gateway applique les politiques de sécurité en ligne sur le chemin des requêtes, pendant toute la durée de la session et pour chaque appel d'outil. Les travaux de recherche indépendants du Dr Chase Cunningham et d'Anthropic sont parvenus à la même architecture que celle déjà développée par Cequence.

Accès à privilège minimal avec Agent Personas

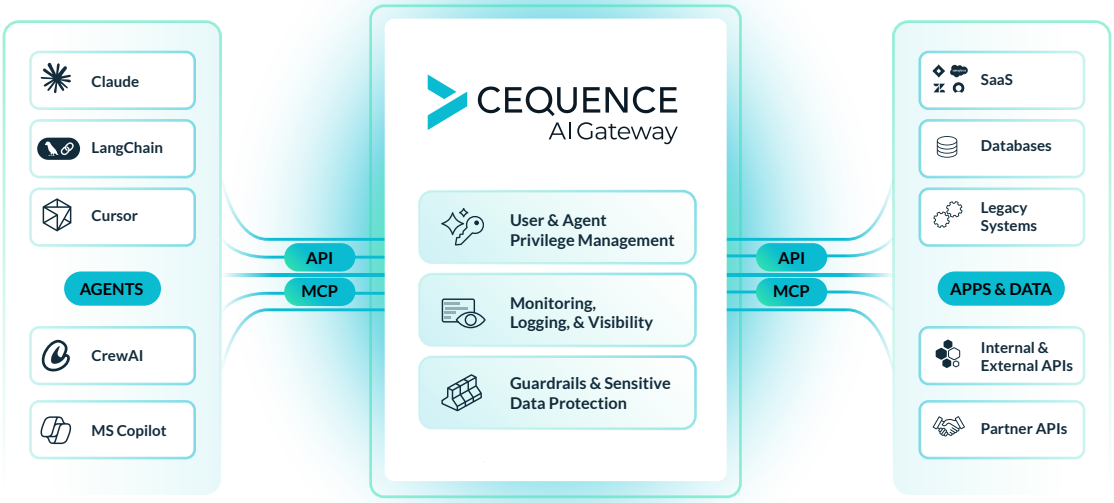
Une description de mission rédigée en langage naturel est transformée en rôle « deny-by-default » avec des autorisations définies pour chaque appel d'outil : outils MCP spécifiques, opérations API et objets de données autorisés, et rien de plus. Les Personas sont opérationnelles dès le premier appel d'outil, sans phase d'apprentissage préalable.

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.

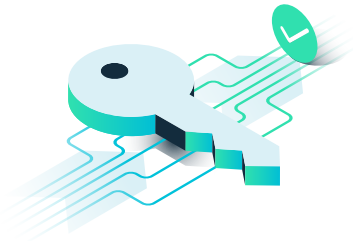


Cequence AI Gateway fournit la sécurité et la gouvernance dont les entreprises ont besoin pour déployer en toute confiance des workflows d'IA agentique à grande échelle.

Fonctionnalités d'AI Gateway

Gestion des identités et des accès des agents

Agent Personas. Chaque agent reçoit une description de mission qui détermine son accès aux outils. Cette gouvernance est assurée par un Skill Registry centralisé qui définit quelles compétences sont associées à quelles Personas. Chaque Persona est associée à un point d'accès virtuel unique et les contrôles sont appliqués en ligne par l'AI Gateway. Les Agent Personas n'exposent que les outils nécessaires à leur mission. L'agent reçoit ainsi une liste restreinte d'outils plutôt que plusieurs centaines à chaque requête, ce qui réduit la consommation de tokens et améliore les performances en permettant au modèle de sélectionner le bon outil dès la première tentative.



Isolation des identifiants. L'agent s'authentifie auprès du gateway à l'aide d'un identifiant qui lui donne accès au gateway uniquement. L'agent et le modèle n'ont jamais accès aux secrets des systèmes backend, empêchant ainsi un agent compromis ou un prompt manipulé d'exposer les identifiants de vos systèmes.

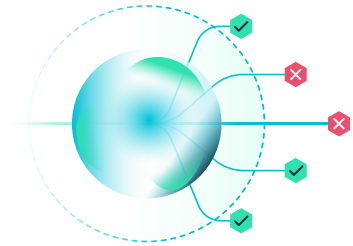
Authentification d'entreprise. Prise en charge de plusieurs fournisseurs d'identité avec OAuth 2.1, PKCE, enregistrement dynamique, intégration OIDC et compatibilité avec les mécanismes d'authentification hérités, afin de garantir le respect des politiques d'identité et d'autorisation de l'entreprise pour les identités humaines comme non humaines.

Gouvernance et conformité

Supervision et visibilité. Chaque requête enregistre l'agent, l'utilisateur, l'outil utilisé, l'horodatage et le résultat obtenu, créant ainsi une piste d'audit inaltérable répondant aux exigences des référentiels de conformité et des processus de réponse aux incidents. Les données et journaux peuvent être exportés au format OTEL pour intégration avec les plateformes SIEM et GRC.

Protection des données sensibles. Une action peut satisfaire aux contrôles d'autorisation tout en permettant l'exfiltration de données sensibles. C'est pourquoi le gateway inspecte chaque requête et chaque réponse en transit. Il bloque les transferts de données sensibles entre outils autorisés, détecte les collectes progressives de données en les comparant aux références comportementales de chaque Persona, masque les identifiants présents dans les arguments des outils et empêche les données de production d'être envoyées vers des environnements de développement ou des outils externes. L'intégration avec les infrastructures DLP existantes est simple et immédiate.

Sécurité



Détection des anomalies comportementales. Des références comportementales sont établies pour chaque Persona, utilisateur et outil afin d'identifier les schémas que l'analyse d'appels individuels ne peut détecter. Un agent qui consulte 200 tickets d'assistance successivement avant d'ouvrir un outil de messagerie passerait tous les contrôles d'autorisation individuels. Ici, c'est la séquence d'actions elle-même qui constitue la violation. Le gateway peut alors limiter ou interrompre l'activité selon les politiques définies.

Garde-fous et limitations de débit. Limites de débit par agent et par outil, mécanismes de coupure automatique pour les boucles incontrôlées, évaluation automatisée du niveau de risque des outils et contrôles réseau comprenant restrictions IP CIDR, géorestrictions et IP pinning, qui impose l'utilisation des jetons uniquement depuis l'adresse IP à laquelle ils ont été attribués, selon chaque Persona.

Activation

Création de serveurs MCP sans code. Importez une spécification OpenAPI ou Swagger existante, ou sélectionnez parmi les API découvertes au sein de vos applications, puis choisissez les points d'accès à exposer sous forme d'outils. Le gateway génère un serveur MCP en quelques minutes sans développement spécifique. Chaque serveur hérite automatiquement des contrôles de Persona, de la surveillance comportementale et des garde-fous. Déployez-le en mode entièrement géré dans le Cequence Cloud ou en mode autogéré via un chart Helm.

Registre MCP d'entreprise. Éliminez les serveurs MCP non autorisés ou non gouvernés grâce à un catalogue centralisé de serveurs approuvés, construits à partir des API officielles des applications, ainsi que de MCP personnalisés pour vos propres applications. Tous sont provisionnés de manière centralisée avec des capacités IAM intégrées. Le gateway prend en charge les évolutions du protocole MCP, évitant toute modification de code à mesure que le standard évolue.

Éprouvé en production

Un grand opérateur mondial de télécommunications a découvert qu'un agent de développement logiciel utilisé par un développeur légitime avait exécuté une tâche durant un week-end. Après avoir rencontré des dépendances l'empêchant d'achever son travail, l'agent a tenté d'effectuer 2,5 millions d'appels d'outils afin de contourner l'obstacle : création de chemins de fichiers fictifs, manipulation de signatures SHA et recherche de droits d'écriture. Toutes les informations d'authentification étaient pourtant valides. Cequence AI Gateway a détecté ce comportement anormal, alerté les équipes de sécurité et généré l'intégralité de la piste d'audit ainsi que le rapport d'analyse des causes nécessaire à l'investigation.

Conçu pour les entreprises

Déployez la plateforme en mode SaaS avec un tenant dédié à chaque client ou sur site, afin que vos données sensibles ne quittent jamais votre environnement. Les contrôles RBAC, la surveillance continue des environnements et la séparation stricte entre préproduction et production sont fournis en standard. La plateforme est certifiée ISO 27001, conforme PCI DSS et dispose d'une attestation SOC 2 Type II. L'intégration avec Cequence API Security et Bot Management apporte des spécifications API enrichies qui améliorent la précision des agents tout en protégeant contre les attaques, abus et fraudes pilotés par les agents.

Résumé

Toutes les feuilles de route IA convergent vers la même réalité : davantage d'agents, davantage d'autonomie et davantage d'accès aux applications et aux données. Cequence AI Gateway permet de gouverner cette évolution. Chaque agent est provisionné comme un nouvel employé avec un rôle appliquant le principe du moindre privilège et du deny-by-default. Son comportement est surveillé en temps réel par rapport à ce rôle, et les agents dont les actions s'écartent de leur mission sont immédiatement arrêtés. Cequence a co-rédigé le CIS Model Context Protocol Companion Guide et co-préside l'initiative AI-Native Blueprint du TM Forum, contribuant à définir les standards de sécurisation des interactions agentiques. Que vous soyez en phase d'évaluation de plateformes agentiques ou que vous exploitiez déjà des agents en production, Cequence fournit la sécurité, la gouvernance et le contrôle dont les organisations ont besoin.

CEQUENCE

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