CEQUENCE

La loi européenne sur l'intelligence artificielle et Cequence AI Gateway

Aider les entreprises européennes à opérationnaliser leur conformité à l'AI Act de l'UE

L'AI Act de l'UE constitue un risque au niveau du conseil d'administration

Pour les entreprises qui déploient des agents IA, des copilotes, des workflows alimentés par des LLM ou des systèmes autonomes, ce règlement impose des exigences en matière de gouvernance, de transparence, de supervision, de gestion des risques et de responsabilité opérationnelle.

Entré en vigueur le 1er août 2024, l'AI Act sera pleinement applicable à partir d'août 2026. À cette échéance, les organisations déployant des systèmes d'IA à haut risque devront démontrer :

- **Un inventaire et une traçabilité des systèmes d'IA**
- **Une supervision humaine et une responsabilité du déployeur**
- **Une surveillance continue en exploitation et une gestion des risques**
- **Une journalisation prête pour l'audit et la conservation des preuves**
- **Des contrôles de protection et de résidence des données**

Les sanctions en cas de non-conformité peuvent atteindre :

- **35 M€ ou 7 % du chiffre d'affaires annuel mondial pour les pratiques interdites**
- **15 M€ ou 3 % du chiffre d'affaires annuel mondial pour les violations liées aux systèmes à haut risque**

À l'instar du RGPD, l'AI Act de l'UE possède une portée extraterritoriale. Il s'applique donc aux organisations, quel que soit leur lieu d'implantation, dès lors qu'elles mettent des systèmes d'IA sur le marché européen ou que les résultats produits par ces systèmes sont utilisés dans l'Union européenne (notamment sous forme de recommandations, de décisions ou de contenus).

Pourquoi les RSSI ont besoin d'un plan de contrôle de la gouvernance de l'IA

Aujourd'hui, la plupart des entreprises disposent déjà de collaborateurs utilisant des outils d'IA tels que Microsoft Copilot, ChatGPT Enterprise, Claude, Cursor, ainsi que des agents autonomes connectés à des systèmes internes comme GitHub, Salesforce, Jira, Slack, SAP et ServiceNow.

L'enjeu n'est plus simplement de savoir qui a accès à l'IA. L'enjeu est désormais de répondre aux questions suivantes :

Que fait l'agent IA ? À quelles données accède-t-il ? Où ces données sont-elles envoyées ? Et l'organisation est-elle capable de le démontrer aux autorités de contrôle ?

Cequence AI Gateway fournit les couches de sécurité, de contrôle et de gouvernance opérationnelle entre les agents IA et les systèmes de l'entreprise.

Comment Cequence AI Gateway répond aux exigences de l'AI Act de l'UE

Exigence de l'AI Act de l'UE		Capacités de Cequence AI Gateway
Article 9	**Gestion continue des risques**	Surveillance en temps réel, détection d'anomalies, garde-fous, application des politiques, mécanismes d'arrêt d'urgence (« kill switch ») et automatisation de la gouvernance
Article 10	**Gouvernance des données**	Classification des données, surveillance des données sensibles, masquage, expurgation et contrôles régionaux de traitement des données
Article 12	**Conservation des enregistrements**	Pistes d'audit et journaux exportables détaillant l'activité des agents, utilisateurs, applications, appels d'outils et flux de données
Article 13	**Transparence**	Visibilité en temps réel sur le comportement des agents : qui a appelé quoi, quelles données ont été consultées et où elles ont été transmises
Article 14	**Supervision humaine**	Personae d'agents, contrôles d'accès à privilège minimal, mécanismes d'approbation ou de remplacement et capacités d'intervention de type « kill switch »
Article 26	**Obligations des déployeurs de systèmes d'IA à haut risque**	Surveillance du fonctionnement, conservation des journaux, supervision humaine et intervention en cas de détection d'un risque
Article 27	**Évaluation de l'impact sur les droits fondamentaux**	Couche de preuve destinée aux déployeurs devant évaluer les cas d'usage à haut risque grâce aux journaux, à la visibilité des flux de données et aux contrôles de risque
Article 49	**Enregistrement**	Inventaire des agents et systèmes d'IA ainsi que documentation nécessaire à l'enregistrement des systèmes à haut risque

Ce qui distingue Cequence

De nombreuses organisations commencent leur démarche de gouvernance de l'IA par des solutions de gestion des identités et des accès. L'identité répond à la question : « Cet agent IA doit-il recevoir un jeton d'accès ? » Cequence AI Gateway répond à la question : « Que fait l'agent avec cet accès ? »

Cequence offre :

- Une visibilité complète sur les interactions entre l'IA et les applications
- Une surveillance des flux de données sensibles au niveau des échanges
- Des contrôles de gouvernance et d'application des politiques spécifiquement conçus pour l'IA
- Une surveillance continue alignée sur les obligations des déployeurs prévues par l'AI Act
- Des preuves prêtes pour l'audit à destination des autorités, des équipes juridiques et des conseils d'administration

Conçu pour les entreprises

Cequence AI Gateway aide les organisations à déployer l'innovation fondée sur l'IA en toute sécurité tout en réduisant les risques réglementaires, opérationnels et réputationnels.

Pour les RSSI, les responsables de la sécurité et les équipes conformité, Cequence AI Gateway fournit :

- Une gouvernance des agents IA autonomes
- Des capacités d'application des politiques et d'observabilité en temps réel
- Une supervision humaine et une responsabilisation accrues
- Une protection des données sensibles et réglementées
- Une approche pragmatique pour opérationnaliser une IA digne de confiance à l'échelle de l'entreprise

À propos de Cequence Security

Cequence protège les applications et les données qui alimentent les entreprises à l'ère de l'IA agentique. Plus de dix années d'expertise en défense contre les bots et en sécurité des API ont permis à Cequence de s'imposer comme un leader de l'adoption sûre et sécurisée de l'IA agentique.La plateforme Cequence offre une compréhension approfondie du comportement des utilisateurs, des entités et des agents, permettant aux organisations de sécuriser et de contrôler les workflows d'IA agentique tout en se protégeant contre les acteurs malveillants et les agents hors de contrôle. Grâce à une approche sans code et hautement évolutive, Cequence génère de la valeur en quelques minutes plutôt qu'en plusieurs jours ou semaines. Plébiscitée par les organisations privées et publiques les plus exigeantes, Cequence protège plus de 10 milliards d'interactions API par jour et 4 milliards de comptes utilisateurs. Pour en savoir plus, rendez-vous sur cequence.ai

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