CEQUENCE

L'Artificial Intelligence Act dell'Unione Europea e Cequence AI Gateway

Aiutare le imprese europee a rendere operativa la conformità all'AI Act dell'UE

L'AI Act dell'UE rappresenta un rischio a livello di consiglio di amministrazione

L'Artificial Intelligence Act dell'Unione Europea introduce il quadro normativo più completo al mondo in materia di intelligenza artificiale. Per le organizzazioni che implementano agenti AI, copiloti, workflow basati su LLM o sistemi autonomi, il regolamento richiede governance, trasparenza, supervisione, gestione del rischio e responsabilità operativa.

Entrato in vigore il 1° agosto 2024, l'AI Act sarà pienamente applicabile entro agosto 2026. A quel punto, le organizzazioni che utilizzano sistemi di IA ad alto rischio dovranno dimostrare:

- **Inventario e tracciabilità dei sistemi di IA**
- **Supervisione umana e responsabilità del deployer**
- **Monitoraggio continuo in esercizio e gestione del rischio**
- **Registrazione degli eventi pronta per audit e conservazione delle evidenze**
- **Controlli sulla protezione e sulla residenza dei dati**

Le sanzioni per la mancata conformità possono raggiungere:

- **35 milioni di euro o il 7% del fatturato annuo globale per pratiche vietate**
- **15 milioni di euro o il 3% del fatturato annuo globale per violazioni relative ai sistemi ad alto rischio**

Analogamente al GDPR, l'AI Act dell'UE ha portata extraterritoriale. Si applica pertanto alle organizzazioni indipendentemente dalla loro ubicazione fisica qualora immettano sistemi di IA sul mercato europeo o qualora gli output dei loro sistemi siano utilizzati nell'Unione Europea (ad esempio raccomandazioni, decisioni o contenuti).

Perché i CISO hanno bisogno di un piano di controllo per la governance dell'IA

La maggior parte delle imprese dispone già di dipendenti che utilizzano strumenti di IA come Microsoft Copilot, ChatGPT Enterprise, Claude, Cursor e agenti autonomi collegati a sistemi interni quali GitHub, Salesforce, Jira, Slack, SAP e ServiceNow.

La sfida non consiste più semplicemente nel sapere chi ha accesso all'IA. La vera domanda è:

> **Che cosa ha fatto l'agente AI? A quali dati ha avuto accesso? Dove sono stati trasferiti tali dati? E l'organizzazione è in grado di dimostrarlo alle autorità di regolamentazione?**

Cequence AI Gateway fornisce i livelli di sicurezza, controllo e governance operativa tra gli agenti AI e i sistemi aziendali.

Come Cequence AI Gateway supporta la conformità all'AI Act dell'UE

Requisito dell'AI Act UE		Capacità di Cequence AI Gateway
Articolo 9	**Gestione continua del rischio**	Monitoraggio runtime, rilevamento delle anomalie, guardrail, applicazione delle policy, controlli di kill switch e automazione della governance
Articolo 10	**Governance dei dati**	Classificazione dei dati, monitoraggio dei dati sensibili, mascheramento, redazione e controlli regionali sul trattamento dei dati
Articolo 12	**Conservazione delle registrazioni**	Audit trail e log esportabili che mostrano attività di agenti, utenti, applicazioni, chiamate agli strumenti e flussi di dati
Articolo 13	**Trasparenza**	Visibilità in tempo reale sul comportamento degli agenti: chi ha richiamato cosa, quali dati sono stati consultati e dove sono stati trasferiti
Articolo 14	**Supervisione umana**	Personae degli agenti, controlli di accesso a privilegio minimo, meccanismi di approvazione o override e controlli di intervento di tipo kill switch
Articolo 26	**Obblighi dei deployer di sistemi di IA ad alto rischio**	Monitoraggio operativo, conservazione dei log, supervisione umana e intervento in presenza di rischi
Articolo 27	**Valutazione dell'impatto sui diritti fondamentali**	Livello di evidenza per i deployer che devono valutare casi d'uso ad alto rischio tramite log, visibilità dei flussi di dati e controlli del rischio
Articolo 49	**Registrazione**	Inventario di agenti e sistemi AI e documentazione necessaria per la registrazione dei sistemi ad alto rischio

Cosa rende Cequence diversa

Molte organizzazioni iniziano il proprio percorso di governance dell'IA con strumenti di Identity and Access Management. L'identità risponde alla domanda: "Questo agente AI dovrebbe ricevere un token di accesso?" Cequence AI Gateway risponde invece alla domanda: "Che cosa ha fatto l'agente con quell'accesso?"

Cequence offre:

- Visibilità completa sulle interazioni tra IA e applicazioni
- Monitoraggio dei flussi di dati sensibili a livello di traffico
- Controlli di governance e applicazione delle policy specifici per l'IA
- Monitoraggio continuo allineato agli obblighi dei deployer previsti dall'AI Act
- Evidenze pronte per gli audit destinate a regolatori, team legali e consigli di amministrazione

Progettato per le imprese

Cequence AI Gateway aiuta le organizzazioni a rendere sicura l'innovazione basata sull'IA riducendo al contempo i rischi normativi, operativi e reputazionali.

Per CISO, responsabili della sicurezza e team di compliance, Cequence AI Gateway offre:

- Governance degli agenti AI autonomi
- Enforcement runtime e osservabilità completa
- Supervisione umana e responsabilizzazione
- Protezione dei dati sensibili e regolamentati
- Un percorso concreto per rendere operativa una "IA affidabile" su scala enterprise

Informazioni su Cequence Security

Cequence protegge le applicazioni e i dati che alimentano le imprese nell'era dell'IA agentica. Oltre dieci anni di esperienza nella difesa dai bot e nella sicurezza delle API hanno reso Cequence un punto di riferimento nell'adozione sicura dell'IA agentica. La piattaforma Cequence offre una comprensione approfondita del comportamento di utenti, entità e agenti, consentendo alle organizzazioni di proteggere e controllare i workflow di IA agentica difendendosi al contempo da attori malevoli e agenti fuori controllo. Grazie a un approccio altamente scalabile e senza codice, Cequence genera valore in pochi minuti anziché in giorni o settimane. Scelta da alcune delle organizzazioni pubbliche e private più grandi ed esigenti al mondo, Cequence protegge oltre 10 miliardi di interazioni API al giorno e 4 miliardi di account utente. Per ulteriori informazioni, visita cequence.ai

CEQUENCE

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