CEQUENCE

The EU Artificial Intelligence Act and Cequence AI Gateway

Helping European Enterprises Operationalise EU AI Act Compliance

The EU AI Act Is a Board-Level Risk

The European Union AI Act introduces the world's most comprehensive regulatory framework for artificial intelligence. For enterprises deploying AI agents, copilots, LLM-powered workflows, or autonomous systems, the Act requires governance, transparency, oversight, risk management, and operational accountability.

The EU Act, in effect since 01 August 2024, goes into full force by August 2026, when organizations deploying high-risk AI systems must demonstrate:

- **AI system inventory and traceability**
- **Human oversight and deployer accountability**
- **Continuous runtime monitoring and risk management**
- **Audit-ready logging and evidence retention**
- **Data protection and residency controls**

Non-compliance penalties can reach:

- **€35M or 7% of global annual turnover** for prohibited practices
- **€15M or 3% of global annual turnover** for high-risk system violations

Note that like the GDPR, the EU AI Act has extraterritorial reach. So, the act applies to organizations regardless of where they are physically located if they are placing AI systems on the EU market or their AI system's output is used in the EU (including such as recommendations, decisions, or content).

Why CISOs Need an AI Governance Control Plane

Most enterprises already have employees using AI tools such as Microsoft Copilot, ChatGPT Enterprise, Claude, Cursor, and autonomous agents connected to internal systems including GitHub, Salesforce, Jira, Slack, SAP, and ServiceNow.

The challenge is no longer simply *who has access to AI.*

The challenge is:

> **What did the AI agent do, what data did it access, where did the data go, and can the organization prove it to regulators?**

Cequence AI Gateway provides the security, control, and operational governance layers between AI agents and enterprise systems.

How Cequence AI Gateway Aligns to the EU AI Act

EU AI Act Requirement		Cequence AI Gateway Capability
Article 9	**Continuous risk management**	Runtime monitoring, anomaly detection, guardrails, policy enforcement, kill-switch controls, and governance automation
Article 10	**Data governance**	Data classification, sensitive data monitoring, masking, redaction, and regional data handling controls
Article 12	**Record-keeping**	Audit trails and exportable logs showing agent, user, app, tool-call, and data-flow activity
Article 13	**Transparency**	Real-time visibility into agent behaviour – who called what, what data was accessed, and where it went.
Article 14	**Human oversight**	Agent Personas, least-privilege access controls, approval/override patterns, and kill-switch style intervention controls
Article 26	**Obligations of Deployers of High-Risk AI Systems**	Monitoring of operation, retained logs, human oversight, and intervention when risk is detected
Article 27	**Fundamental Rights Impact Assessment**	Evidence layer for deployers that must assess high-risk use cases, especially through logs, data-flow visibility, and risk controls
Article 49	**Registration**	AI/agent inventory and documentation needed for high-risk system registration

What Makes Cequence Different

Many organizations begin AI governance with identity and access management tools. Identity answers, "Should this AI agent receive a token?" Cequence AI Gateway answers, "What did the agent do with that access?"

Cequence delivers:

- Full runtime visibility across AI-to-application interactions
- Flow-level monitoring of sensitive data movement
- AI-specific governance and enforcement controls
- Continuous monitoring aligned to deployer obligations under the EU AI Act
- Audit-ready evidence for regulators, legal teams, and boards

Designed for Enterprises

The Cequence AI Gateway helps organizations safely operationalize AI innovation while reducing regulatory, operational, and reputational risk. For CISOs, security leaders, and compliance teams, the Cequence AI Gateway provides:

- Governance for autonomous AI agents
- Runtime enforcement and observability
- Human oversight and accountability
- Protection of sensitive and regulated data
- A practical path to operationalizing "trustworthy AI" at enterprise scale

About Cequence

Cequence protects the applications and data that power enterprises in the agentic era. More than a decade of bot defence and API security experience has established Cequence as the leader of safe and secure agentic AI adoption. The Cequence platform delivers deep insight into user, entity, and agent behaviour, enabling organizations to secure and control agentic AI workflows while protecting against bad actors and rogue agents. Cequence delivers value in minutes rather than days or weeks with a highly scalable, no-code approach. Trusted by the largest and most demanding private and public sector organizations, Cequence protects more than 10 billion daily API interactions and 4 billion user accounts. Learn more at cequence.ai.

CEQUENCE

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