SALT

The EU AI Act: Ensuring Trustworthy AI

Navigating AI Compliance and Security with API Governance

The EU AI Act is a landmark legal framework that establishes harmonized, risk-based rules for AI systems in the EU. For high-risk systems, the Act mandates rigorous requirements that directly impact the APIs serving them. Since APIs are the primary interfaces to AI, their security and governance are essential for meeting the Act's stringent compliance demands.

Risk-Based Approach:

- **Prohibited AI:** Bans AI practices that pose an unacceptable risk, such as social scoring by public authorities.
- **High-Risk AI:** Imposes strict requirements on AI systems used in critical sectors like medical devices, critical infrastructure, law enforcement, and employment.
- **Limited-Risk AI:** Requires transparency for systems like chatbots or deepfakes to ensure users know they are interacting with AI.
- **Minimal-Risk AI:** Enables the free use of minimal-risk AI systems, like AI-enabled video games, subject to voluntary codes of conduct.

Data and Data Governance:

- High-risk AI systems must be trained and validated on high-quality, relevant, and representative data.
- Securing the APIs that serve as data conduits is fundamental to ensuring data quality and preventing data poisoning.
- The Act also requires data governance to prevent bias and ensure secure handling throughout the data lifecycle.

Robustness, Accuracy, and Security:

- High-risk AI systems must be accurate and resilient against errors, faults, or inconsistencies.
- Systems require appropriate cybersecurity to protect them from malicious third parties attempting to alter their use or performance.
- This directly implicates API security, as APIs represent the primary attack surface.

The EU AI Act: Ensuring Trustworthy AI

Why It Matters:

The EU AI Act sets a global precedent for AI regulation, impacting any organization with AI systems in the EU market. Compliance is mandatory, with significant fines up to €35 million or 7% of global turnover. Adherence ensures market access and builds user trust by demonstrating that AI services are safe, transparent, and ethical.

API Security Requirements:

- **Secure and Resilient APIs:** APIs must be resilient against attacks that could compromise the AI system's performance, availability, or security.
- **Data Integrity and Confidentiality:** APIs must use strong encryption and access controls to protect data integrity and confidentiality for high-risk AI.
- **Logging and Traceability:** API interactions for high-risk systems must be logged to ensure traceability and human oversight per the Act.

Relevant Articles Where API Security is a Critical Underlying Control:

- **Article 10 (Data and Data Governance):** API security is crucial to ensure quality, integrity, and secure handling of data for high-risk systems.
- **Article 15 (Accuracy, robustness, and cybersecurity):** Mandates cybersecurity for high-risk systems, making API security fundamental to compliance.
- **Articles 12 & 20 (Technical Documentation & Traceability):** Require comprehensive observability and immutable logging to ensure continuous traceability across all AI agent actions and API interactions.

How Salt Security Helps:

Salt Security provides the verifiable technical controls required for compliance with the EU AI Act. Utilizing the **Agentic Security Graph,** Salt establishes a centralized system of record that delivers complete visibility and observability across all AI-to-API interactions. This continuous discovery identifies every interface connecting to high-risk AI systems. Posture governance enforces strict access controls to meet the Act's cybersecurity mandates. By providing deep observability into data flows, Salt ensures data governance and prevents unauthorized access. Finally, behavioral threat protection stops logic attacks that could alter AI behavior, providing immutable evidence of system resilience.

Learn more about API Security and Compliance in our whitepaper.