JFROG PLATFORM:
CYBER RESILIENCE ACT (CRA) COMPLIANCE BRIEF

European Union Agency for Cybersecurity

Overview

The European Union's Cyber Resilience Act (CRA) is an established law (Regulation EU 2024/2847) that ensures products with digital elements are designed, developed, and maintained securely throughout their lifecycle. While the regulation entered into force in December 2024, its enforcement is phased: mandatory 24-hour reporting obligations take effect on September 11, 2026, and full compliance is required by December 11, 2027. This upcoming mandate transforms software security from a best practice into a strict legal requirement. Manufacturers face strict liability and penalties of up to €15 million or 2.5% of global turnover for non-compliance. To secure EU market access and maintain the mandatory CE Mark, organizations must shift from manual audits to automated, continuous security across their entire software supply chain.

How JFrog helps organizations with meeting CRA obligations

JFrog provides an end-to-end Secure Software Supply Chain Platform that serves as your single system of record for automating, managing, securing, and governing all binary artifacts. Acting as your ultimate trust layer, the platform's built-in security and governance tooling — including JFrog Curation, Xray, Advanced Security, Runtime, and AppTrust — equips organizations to meet the CRA's strict mandates natively. Together, these solutions enable continuous compliance without massive manual audit overhead.

CRA Key Facts

- **Covered Products:** Hardware and software with digital elements that can connect to networks, either directly or indirectly.
- **Affected Entities:** Any company (EU or non-EU) manufacturing, importing, or selling digital products (including internally developed software) within the European market. These organizations face strict liability and penalties of up to €15 million or 2.5% of global turnover, making CRA compliance a strict business prerequisite to defend EU market access.
- **The CE Mark:** Products must complete required security assessments to bear the CE mark and be legally sold in the EU.
- **High-Risk Tiers:** The CRA applies risk-based categories. Security and supply chain tools fall into the stricter Class I ("Important") category, subjecting them to the highest compliance mandates.
- **Open-Source Liability:** Non-profit OSS stewards face lighter rules, but commercial manufacturers remain strictly liable for integrated open-source components, requiring automated governance.

CRA Core Requirements

The CRA requires companies to adopt secure development practices, proactively manage vulnerabilities, and maintain comprehensive auditability. Compliance is a non-negotiable prerequisite for EU market access, enabling products to be secure and trusted.

Security by Design

Products must be designed and developed with security as a core consideration

Risk Management

Continuous risk assessment and mitigation throughout the product lifecycle

Vulnerability Handling

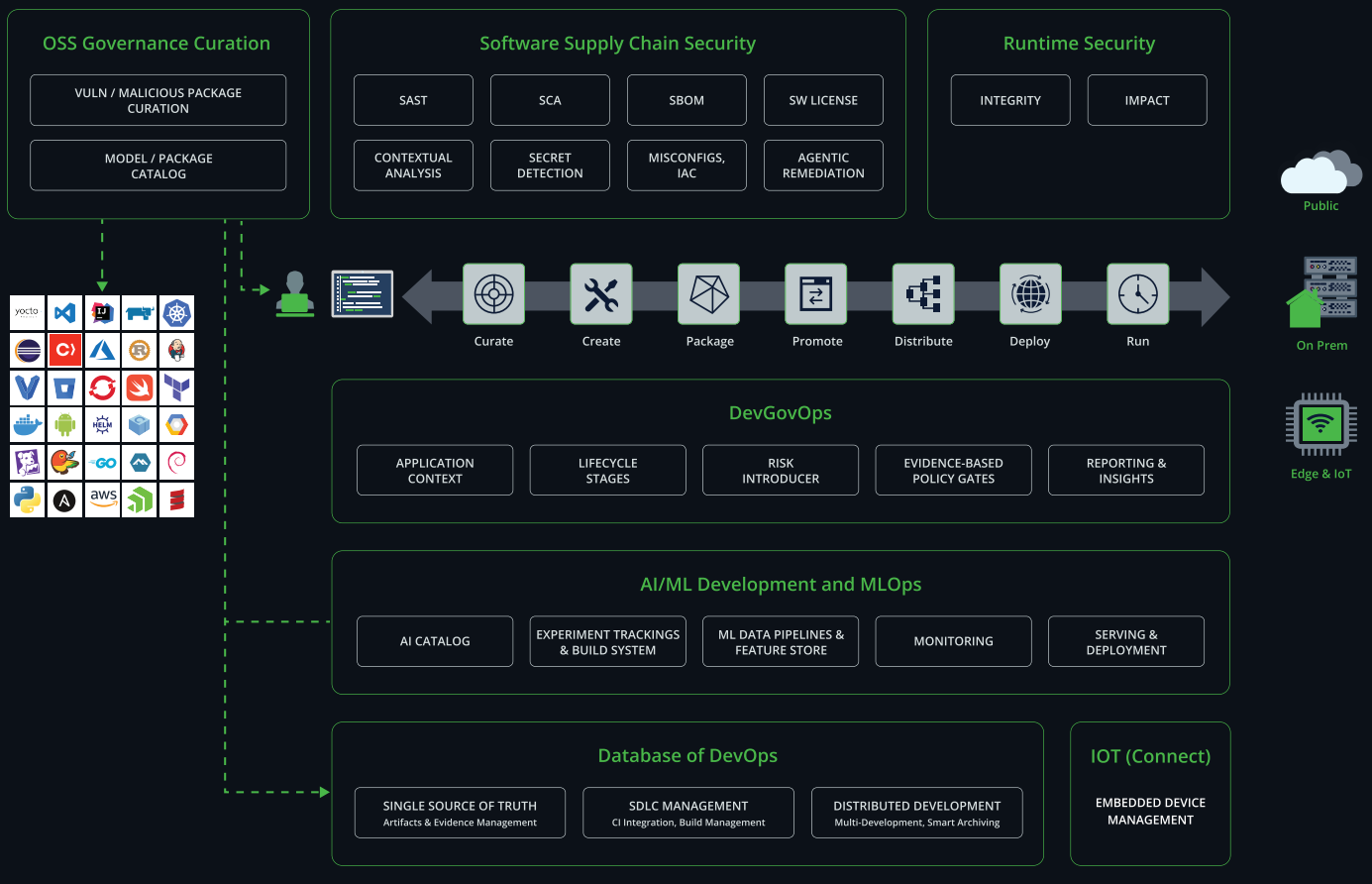
Identification, 24-hour reporting of actively exploited vulnerabilities, rapid remediation, SBOMs

Regular Updates

Products must receive regular security updates to address new vulnerabilities without delay

Scanners check code, but the CRA regulates the product you ship: the binary. The JFrog Platform is a unified solution for secure, controlled software delivery from code to runtime — securing binary artifacts and generating mandatory SBOMs to create an immutable single source of truth. This bridges the gap between development, operations, and security teams, scaling trust at the speed of modern software delivery.

The JFrog Software Supply Chain Platform



JFrog Curation, Catalog and IDE Plugins

Establish a secured environment to satisfy the CRA's strict liability mandates and a Security by Design foundation.

- **Secure by Design Enforcement:** Automatically block unsafe or highly vulnerable open-source packages at the front door before they enter your software supply chain.
- **Third-Party Due Diligence:** Mitigate strict liability risks by establishing a “clean pipe” environment that ensures third-party components do not compromise product cybersecurity.
- **Shift-Left Resolution:** Utilize IDE plugins to empower developers to identify and resolve vulnerabilities directly at their desks, maintaining continuous compliance without slowing down delivery velocity.

JFrog Xray, Advanced Security and Runtime

Detect and remediate vulnerabilities early to meet the CRA's strict incident reporting requirements and track SLAs.

- **Automated SBOMs & VEX:** Generate mandatory machine-readable SBOMs enriched with VEX (Vulnerability Exploitability eXchange) data to fulfill the CRA's strict product documentation requirement and minimum 5-year vulnerability tracking mandate per release.
- **Contextual Analysis:** Solves the prioritization paradox by identifying genuinely exploited CVEs, empowering your team to hit CRA's strict ENISA reporting deadlines, providing automated alerting to meet the notification mandates: 24-hour early warnings, 72-hour detailed notifications, and 1-month final reports.
- **Secure by Design Infrastructure:** Ensure your deployments meet the CRA's 'Security by Design' configuration mandates by continuously scanning Infrastructure-as-Code (IaC).

JFrog AppTrust

Automate CRA compliance and continuous governance by eliminating manual bottlenecks with a legally defensible system of record.

- **Release Lifecycle Management:** Provides a structured promotion flow that physically moves immutable application bundles through defined stages, guaranteeing only audit-verified releases reach production.
- **Automated Evidence Collection:** Consolidates security, quality, performance and releasing evidence into a single source of truth, cryptographically binding it to your binaries for a tamper-proof chain of custody.
- **Policy as Code (PaC):** Translates complex CRA regulations into executable Open Policy Agent (OPA) code to enforce automated release gates that proactively block non-compliant software.

CRA Compliance Starts Here

The JFrog Platform embeds governance, risk, and compliance (GRC) directly into development workflows via a DevGovOps approach. AppTrust evidence-based release gates replace manual audit overhead with continuous, automated CRA adherence without sacrificing delivery velocity.

See it in action. Schedule a Demo

www.jfrog.com

www.x.com/jfrog

www.facebook.com/artifrog/

www.linkedin.com/company/jfrog-ltd