



CYBER RESILIENCE ACT (CRA) JFROG PLATFORM COMPLIANCE BRIEF

ABSTRACT

The European Union's Cyber Resilience Act (CRA) is an enacted law (Regulation EU 2024/2847) ensuring that 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 took 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 ensure continuous compliance without massive manual audit overhead.

CRA SCOPE & IMPACT

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 within the European market.
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.

Platform Compliance Mapping

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, ensuring products are 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

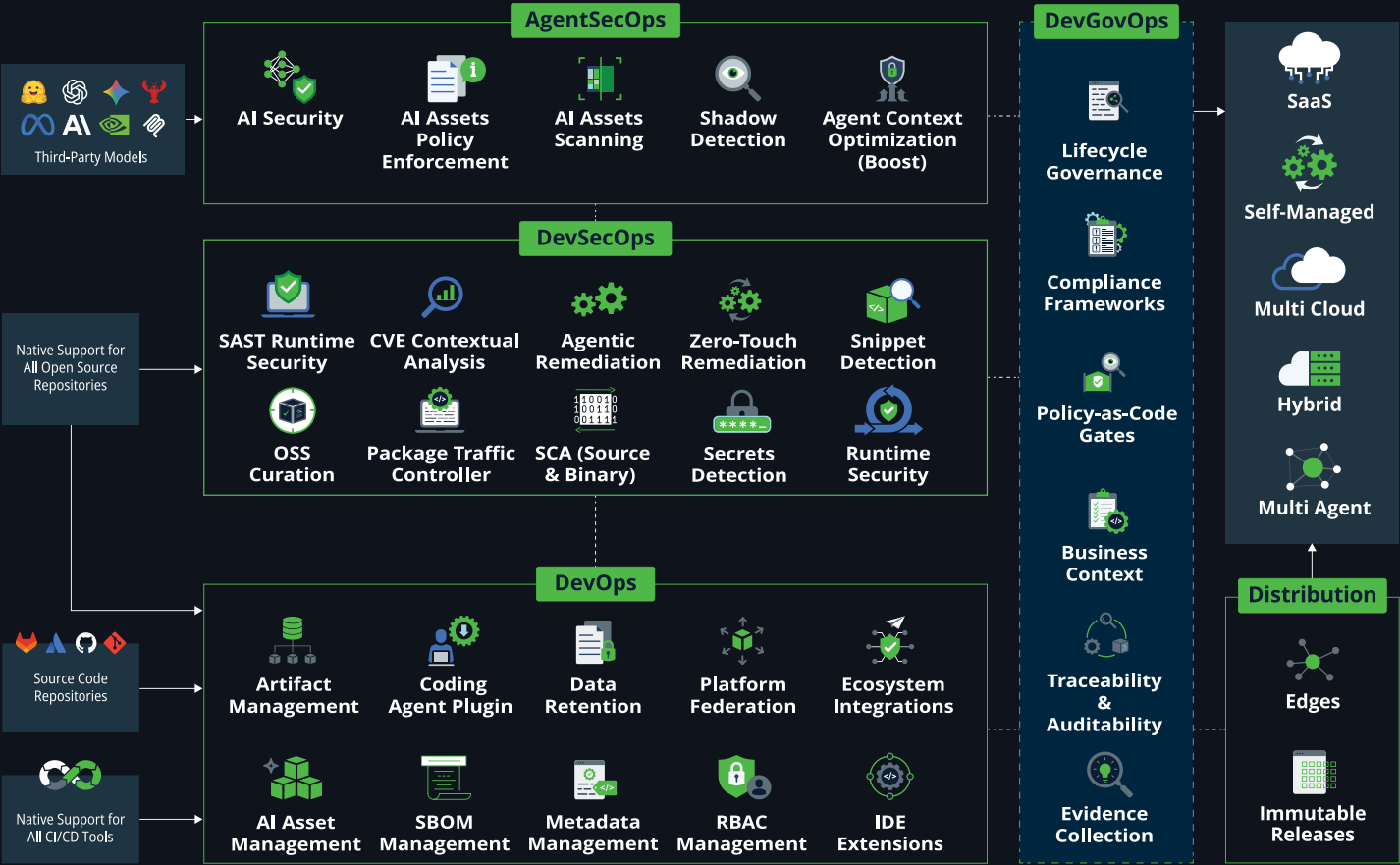
VULNERABILITY HANDLING

Mandatory mechanisms for the identification, 24-hour reporting, and rapid remediation of vulnerabilities

REGULAR UPDATES & PATCHES

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

The JFrog Platform is a unified solution that ensures secure and controlled software delivery from code to runtime. Scanners check code, but the CRA regulates the product you ship - the binary. JFrog acts as your ultimate Trust Layer, securing the binary artifacts to provide an immutable single source of truth. This bridges the gap between developers, operations, and security teams, scaling trust at the speed of modern development.



JFrog Curation, Catalog & IDE Plugins

Establish a secured environment to satisfy the CRA's Strict Liability mandates and a Secure-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 & Runtime

Detect and remediate vulnerabilities early to meet the CRA's strict incident reporting and tracking 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 its minimum 5-year vulnerability tracking mandate per release.
- **Contextual Analysis:** Solves the prioritization paradox by identifying genuinely exploitable CVEs, empowering your team to hit CRA's strict ENISA reporting deadlines: 24-hour early warnings, 72-hour detailed notifications, and 1-month final reports.
- **Secure-by-Default Infrastructure:** Ensure your deployments meet the CRA's 'Secure-by-Default' 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.

- **Lifecycle Governance:** Provides a structured promotion flow that physically moves immutable application bundles through defined stages, so you can prove to auditors that only verified releases reached production.
- **Automated Evidence Collection:** Automatically 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.
- **Pre-Mapped Policy as Code (PaC):** Enforce CRA compliance without manual policy writing. AppTrust applies pre-mapped CRA frameworks directly to Open Policy Agent (OPA) release gates out of the box, delivering real-time compliance coverage scoring while proactively blocking non-compliant software across the SDLC.

JFrog's integrated platform provides comprehensive risk assessments, eliminates vulnerability noise, and maintains immutable audit trails. By leveraging the platform's integrated security capabilities and embracing a DevGovOps approach - embedding governance, risk, and compliance (GRC) directly into development workflows - businesses can replace massive manual audit overhead with automated evidence-based gates using JFrog AppTrust. This guarantees **continuous compliance** with the Cyber Resilience Act while safely accelerating software delivery.

[Request a Demo](#)

To learn more about how the JFrog platform can help you meet these critical requirements.

ABOUT JFROG

JFrog empowers thousands of DevOps organizations globally to build, secure, distribute, and connect any software artifact to any environment using the universal, hybrid, multi-cloud JFrog Platform.



LEGAL STATEMENT

Copyright © 2026 JFrog LTD. JFrog, the JFrog logo, and JFrog Artifactory are trademarks or registered trademarks of JFrog LTD or its subsidiaries in the United States and other countries. All other marks and names mentioned herein may be trademarks of their respective companies.



www.jfrog.com



www.x.com/jfrog



www.facebook.com/artifrog/



www.linkedin.com/company/jfrog-ltd