

WHITEPAPER

EU Cyber Resilience Act & Mythos: Securing Your Container Infrastructure with RapidFort

How a new generation of AI vulnerability discovery tools, including models like Claude Mythos, is reshaping enterprise security and what your container teams must do now.

Container Security

EU Compliance

AI Threat Response

Dec 2027

Full CRA enforcement for all products in EU markets

Sep 2026

Reporting obligations begin under Article 14

24 Hours

CSIRT and ENISA early warning for active exploits

TABLE OF CONTENTS

- 01 Introduction
- 02 What the CRA Covers in Cloud-Native Environments
- 03 The Mythos Era: AI and the New Vulnerability Threat
- 04 Three CRA Requirements Every Container Team Must Know
- 05 How the CRA Affects Your Kubernetes Cluster
- 06 How to Prepare: Four Practical Steps
- 07 How RapidFort Helps You Meet CRA Requirements

Who Should Read This Whitepaper

Written for security and engineering leaders, including CISOs, DevSecOps teams, platform engineers, and compliance officers responsible for cloud-native workloads distributed to EU markets.

AT A GLANCE

Regulation	EU Cyber Resilience Act (Regulation (EU) 2024/2847)
In Force	December 10, 2024
Reporting Begins	September 11, 2026
Full Enforcement	December 11, 2027
Scope	Container images, Kubernetes operators, and Helm charts distributed commercially to EU markets
Key Obligations	Security by design, ongoing vulnerability management with SBOM documentation, five-year minimum support period
Reporting Windows	24-hour and 72-hour notifications to the CSIRT coordinator and ENISA; 14-day final report once corrective or mitigating action is available

RapidFort in Numbers

Up to 99.9%

Vulnerability Elimination

Achievable in hours, not months

Up to 90%

Attack Surface Reduction

Without code changes

7 of 10

Top AI Companies

Across customer deployments

01 Introduction

The EU Cyber Resilience Act (CRA) sets mandatory cybersecurity standards for every product with digital elements sold in EU markets. It came into force on December 10, 2024, with incident reporting obligations starting September 11, 2026, and full enforcement from December 11, 2027.

For container and cloud-native teams, the CRA is not a distant concern. It shapes how cloud-native applications are built, distributed, and maintained. This guide explains what compliance requires and how AI tools like Mythos make urgency unavoidable.



Figure 1: CRA Enforcement Timeline

02 What the CRA Covers in Cloud-Native Environments

Commercially supplied container images, Kubernetes operators, Helm charts, and other software components may fall within the CRA when they qualify as products with digital elements or integrated components made available on the EU market.

Open-source software is only in scope when distributed commercially. Non-commercial open-source projects are exempt, though organisations that systematically monetise such projects may carry obligations as software stewards under Article 24.

Within CRA Scope	Key Nuances
Container Images Commercially distributed to EU markets	Product Reach Where your users are, not where you are based
Kubernetes Operators Sold or licensed as a commercial product	EU Customer Access Having EU users triggers CRA compliance
Helm Charts With paid support agreements or SLAs	Supply Chain Vendor obligations pass through to you
Open Source Software When embedded in a commercial product	Commercial Terms Paid SLAs and support raise your duties

Figure 2: CRA Scope and Application Nuances

03 The Mythos Era: AI and the New Vulnerability Threat

Anthropic reports that Claude Mythos Preview has demonstrated advanced vulnerability-discovery capabilities across major operating systems, browsers, and open-source projects; treat this as an emerging but credible signal that timelines are compressing, as independent validation of its full scope remains limited.

If such capabilities scale as described, discovery could span a broader surface and map how individual flaws chain into exploit paths, meaning a list of CVEs may represent compounding rather than linear risk.

Discovery Is Scaling

AI systems surface security flaws faster and across far broader code bases than human researchers, at a pace no traditional patch cycle was designed to match.

Remediation Is Not

Patching, validation, and deployment still run at human speed. The gap between known vulnerabilities and fixed ones grows wider every day.

What This Means for Your Container Environment

Base images, system libraries, and open-source dependencies inside Kubernetes clusters are exactly the kind of long-lived, widely-deployed code that AI discovery tools target first. Vulnerabilities quiet in production for years are now being found faster than any patch process was designed to handle.

The Remediation Gap

The CRA's 24-hour reporting window to the CSIRT coordinator and ENISA, continuous SBOM obligations, and five-year support requirements were designed precisely for this gap between discovery and remediation. Reacting to vulnerabilities as they surface is no longer a defensible posture. Reducing the software attack surface is the only answer.

Is Your Environment Ready for Mythos?

Anthropic reports that Claude Mythos Preview is compressing vulnerability-discovery timelines while enterprise patching still lags at 30 to 45 days, though independent validation of these capabilities remains limited. RapidFort's Mythos Readiness Assessment gives you a clear, prioritised view of your true exposure with no code changes required and actionable results within minutes.

[Request Your Free Mythos Readiness Assessment](#) ↗

04 Three CRA Requirements Every Container Team Must Know

The CRA introduces three categories of obligations that directly affect how container infrastructure is built, monitored, and maintained.

01

Security by Design

Hardened base images, minimal software attack surface, and secure defaults as legal requirements, not recommendations.

02

Vulnerability Management

SBOM documentation, continuous monitoring, and 24-hour reporting to the CSIRT coordinator and ENISA for actively exploited vulnerabilities.

03

Long-Term Security

Security updates, rebuild pipelines, and backward-compatible patching for a minimum of five years from first release.

Security by Design and Default

The CRA requires base images to be hardened, with unnecessary components removed and secure configurations applied, before products reach the market. What the cloud-native community has long recommended as best practice is now a legal obligation.

Vulnerability Management and Incident Reporting

Under Article 14, your team must maintain an SBOM, monitor continuously for vulnerabilities, and meet strict notification timelines when actively exploited vulnerabilities are discovered:

24h

EARLY WARNING

Initial notice to the CSIRT coordinator and ENISA via the single reporting platform

72h

VULNERABILITY REPORT

Detailed product, exploit, and mitigation information

14d

FINAL REPORT

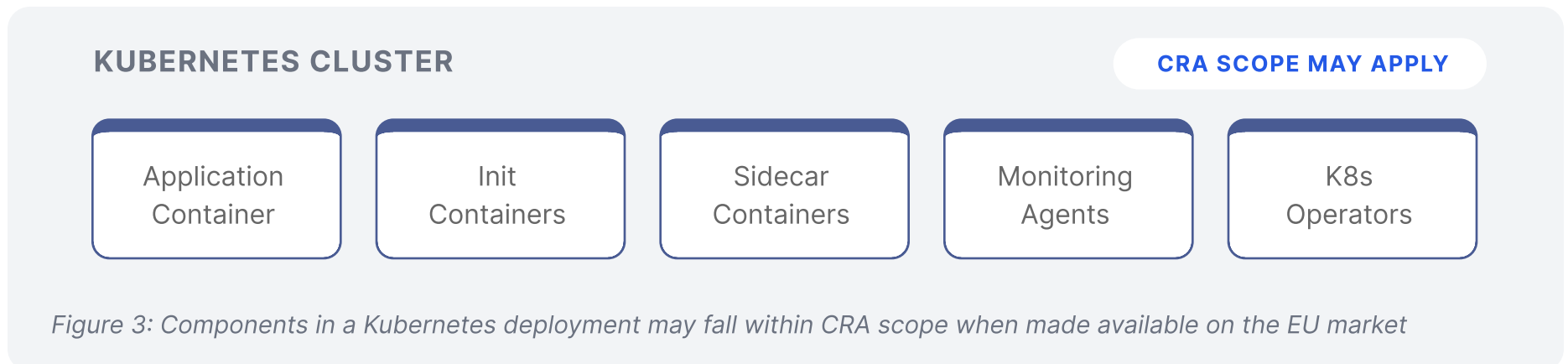
Final report after a corrective or mitigating measure is available; severe incidents carry a separate one-month timeline

Long-Term Security: The Five-Year Commitment

The CRA requires security update support for the full life of your product, at minimum five years from first release. This means tracking which container versions your customers run, keeping rebuild pipelines active for older images, and ensuring fixes can be applied without breaking compatibility.

05 How the CRA Affects Your Kubernetes Cluster

A typical Kubernetes production deployment pulls container images from many sources, each with its own security practices and update cadence. Where those components qualify as products with digital elements made available on the EU market, CRA obligations may apply.



If your product integrates third-party operators, controllers, or images, you may have due-diligence and vulnerability-management obligations for the integrated product. The supplier's own CRA obligations remain separate.

06 How to Prepare: Four Practical Steps

These four areas give any cloud-native team a practical starting point for CRA readiness.

01 Minimal Containers

Start from secure, hardened base images with no inherited vulnerabilities. Remove unnecessary software to reduce the software attack surface before reaching production.

02 SBOM Complemented with RBOM®

Add runtime profiling to distinguish what is installed from what actually executes. RapidFort's RBOM® can complement your SBOM by showing which components are reachable at runtime, helping prioritise remediation and document risk-based vulnerability handling.

03 Image Distribution Strategy

Know how security updates flow to your users. Ensure registry policies enforce consistent standards across all environments and customer deployments.

04 Supply Chain Visibility

Understand who maintains the images you depend on and how quickly they respond to security issues. Know whether their cadence meets your CRA obligations.

Key Takeaways for Container Teams

The CRA shifts software security from best practice to enforceable product requirement. With AI tools like Mythos accelerating discovery, the window for reactive remediation is closing. Here is what matters most for your teams.



Treat security as a product requirement

A minimal software attack surface and secure defaults are now legal obligations. Non-compliance carries regulatory consequences, not just reputational risk.



Build SBOM and RBOM® hygiene into CI/CD

Pair static SBOM generation with runtime evidence of what actually executes in production. RapidFort's RBOM® complements the SBOM by helping prioritise remediation and document risk-based vulnerability handling.



Operationalise the 24-hour reporting window

Detection and incident response must work at scale across your clusters. If you cannot notify the CSIRT coordinator and ENISA within 24 hours of an actively exploited vulnerability, you are not meeting your Article 14 obligations.



Plan for a five-year support horizon

Every container version distributed to customers needs a rebuild pipeline, a security update pathway, and backward compatibility planning from day one.



Reduce the software attack surface, not just patch

In the age of AI-accelerated discovery, patching cannot keep pace. Eliminating unused code and hardening images at source is the only sustainable approach.

ABOUT RAPIDFORT

RapidFort is a software supply chain security platform that helps enterprises eliminate vulnerabilities at the source. Founded in 2020 and headquartered in Silicon Valley, RapidFort serves over 100 enterprise and public-sector customers, including 7 of the top 10 AI companies, with curated near-zero CVE base images, runtime profiling, and end-to-end software attack surface management. Recognised as a Gartner Cool Vendor in Container Management.

07 How RapidFort Helps You Meet CRA Requirements

RapidFort eliminates vulnerabilities at the source, delivering curated near-zero CVE base images, automated SBOM generation, and RapidFort's RBOM® as a runtime prioritisation layer, achieving up to 99.9% vulnerability reduction with 90% software attack surface reduction, all without code changes.

CRA Requirement	How RapidFort Addresses It
Secure by design and by default	Curated near-zero CVE base images, hardened and continuously patched
SBOM documentation for all components	Automated SBOM generation with up to 25% vulnerability noise reduction
Limit attack surfaces and interfaces	Automated removal of unused code, eliminating up to 99.9% of vulnerabilities
Ongoing vulnerability management 5+ yrs	Audit-ready reports, continuous baseline validation, and evidence trail

Table 1: CRA Requirements Mapped to RapidFort Capabilities

WHY RAPIDFORT FOR CRA READINESS

 CVE Elimination

Up to 99.9% of vulnerabilities eliminated automatically

 Hardened Images

Near-zero CVE, manually patched and continuously scanned

 SBOM and RBOM®

Up to 25% noise reduction; RBOM® adds runtime prioritisation

 Audit Evidence

Continuous baseline validation and evidence trail



Schedule a Call with RapidFort

If your organisation is preparing for CRA compliance and wants to understand how RapidFort can help eliminate vulnerabilities, meet EU regulatory requirements, and stay ahead of AI-accelerated threats like Mythos, speak with our team.

© 2026 RapidFort, Inc.

Eliminate attack vectors at the source

Schedule a Call ➔

www.rapidfort.com | sales@rapidfort.com