traefiklabs

SOLUTION BRIEF • 2026

FRAMEWORK FOUNDATIONS

The EU Cyber Resilience Act and Your Infrastructure Layer

Why CRA compliance is an architectural decision, not a compliance checkbox. How Traefik Labs is building compliant infrastructure by design, not by retrofit.

FOR
Platform, Security & Procurement Leaders

FULL COMPLIANCE
December 11, 2027

REPORTING OBLIGATIONS
September 11, 2026

Compliant infrastructure, by design.

The EU Cyber Resilience Act (CRA) is a landmark regulation designed to improve the cybersecurity of digital products sold or made available on the European market. It applies to Products with Digital Elements (PDEs), including hardware, software, and remote data processing solutions. Software provided purely as a service is covered under NIS2, not the CRA.

> **Why this brief is different.** Most vendor briefs focus on how to help you comply. This one explains how Traefik is CRA-compliant by design. When the CRA asks whether your software supply chain is compliant, you do not need tooling to interpret that question. You need vendors who can answer it directly.

Key Compliance Milestones

Dec 10, 2024	CRA (Regulation 2024/2847) entered into force.
Jun 11, 2026	Member States begin appointing conformity assessment bodies.
Sep 11, 2026	Manufacturers must begin meeting vulnerability and incident reporting obligations.
Dec 11, 2027	Full CRA compliance becomes mandatory for all covered products.

Objectives of the EU CRA

- Strengthen cybersecurity of digital products sold in the EU.
- Increase transparency of cybersecurity risks.
- Align EU practices with global cybersecurity standards.
- Reduce design-stage vulnerabilities in devices and software.
- Clarify liability for breaches by manufacturers and providers.
- Extend CE marking to cover software products.

What the CRA actually requires.

The CRA introduces mandatory requirements for manufacturers, importers, and distributors. Secure-by-design principles, vulnerability management, and long-term support become legal obligations, not best practices. Here is what that means in concrete terms.

Secure by Design

Products must ship with secure defaults, minimized attack surface, least-privilege access controls, and no hardcoded credentials.

Risk-Based Development

Cybersecurity risk assessments required during design, development, and maintenance. Documented and repeatable.

Third-Party Component Due Diligence

Manufacturers must ensure open-source and third-party components meet equivalent security obligations.

Lifecycle Security Updates

Products must receive security updates for at least five years or the expected product lifetime, whichever is shorter.

Vulnerability Management

Documented vulnerability handling policy. Notify ENISA within 24 hours of active exploitation.

Incident Reporting

Severe incidents must be reported to EU authorities (CSIRT + ENISA) within 72 hours, with follow-up reports.

Conformity Assessments

Default products use self-assessment. Important and Critical products require third-party evaluation.

CE Marking

Compliant products must display the CE mark, signaling adherence to CRA standards across the EU market.

Penalties. Non-compliance can attract fines up to **€15 million or 2.5% of global annual turnover**, whichever is higher. For commercial open-source vendors, manufacturer obligations apply in full. The open-source steward exemption covers neutral foundations only.

Compliance evidence, not marketing alignment.

Every CRA requirement is met by concrete architectural choices and operational artifacts. Our commitment is specific, auditable, and ready for your procurement team.

REQUIREMENT	HOW TRAEFIK DELIVERS	ARTIFACT
Secure by Design	Core proxy written in Go, a memory-safe language. Entire classes of vulnerabilities (buffer overflow, use-after-free, heap corruption) eliminated by construction. TLS-by-default, least privilege, no hardcoded credentials.	*Go architecture • default-secure config reference • public threat model*
Risk-Based Development	Threat modeling integrated into release cycle. Security review mandatory for changes to TLS, authN/Z, and routing logic.	*Security review process • risk assessment methodology*
Third-Party Component Due Diligence	SBOM generated per release. Dependencies continuously scanned. Full transitive dependency graph published.	*CycloneDX / SPDX SBOM per release*
Lifecycle Security Updates	Published support policy covering 5+ years of security updates. LTS branches for enterprise customers.	*Public support lifecycle matrix • LTS commitment*
Vulnerability Management	Coordinated vulnerability disclosure policy. Private advisories via GitHub Security Advisories. ENISA-aligned reporting channels.	*security.txt • CVD policy • GHSA feed*
Incident Reporting	Internal playbook aligned to CRA 24h/72h obligations. Direct channels to ENISA and national CSIRTs (starting with CSIRT-FR).	*Incident response runbook • CSIRT contact workflow*
SBOM & Technical Documentation	Every release ships with complete SBOM, signed build provenance (SLSA), and detailed security documentation.	*Signed SBOM • SLSA attestations • public technical docs*
Conformity Assessment Support	Conformity dossier packaged for procurement and audit teams. CE marking preparation underway.	*Customer conformity dossier • CE marking roadmap*

The CRA rewards architectural choices.

The CRA mandates that products be designed to prevent vulnerabilities, not just patch them. Language, governance, and geography become compliance evidence.

Memory safety is not optional

CISA, the FBI, and the NSA have identified memory-unsafe languages (C, C++) as a primary source of critical vulnerabilities in infrastructure software. The CRA's secure-by-design mandate aligns with this guidance.

Traefik

LANGUAGE: GO

Memory-safe by construction. No buffer overflows, no use-after-free, no dangling pointers. The most common class of critical CVEs is eliminated at the language level.

Solo.io / Envoy-based

LANGUAGE: C++

Solo.io Gloo/Kgateway, Tetrate, Istio Ingress, Contour, Ambassador and many others inherit a documented history of memory-safety CVEs: heap use-after-free, buffer overflows, QUIC memory corruption. Each one requires ENISA reporting from Sep 2026.

Kong / F5 / NGINX-based

LANGUAGE: NGINX / LUA / C

NGINX core is C. Lua is memory-safe, but the foundation used by Kong, F5, HAProxy, VMware Avi LB, Citrix, APISIX, and many others inherits the same class of risks as Envoy. The ingress-nginx EoL (March 2025), triggered by IngressNightmare (CVE-2025-1974, CVSS 9.8), exposed the templating-based NGINX config pattern as a systemic risk, not a single bug.

European sovereignty is a procurement factor

Vendor geography becomes a CRA risk input. European vendors with regulatory proximity to ENISA, national CSIRTs, and conformity assessment bodies clear procurement faster than US-based competitors. **Traefik Labs is incorporated in the EU.** CRA is our home regulation.

Bottom Line

Procurement teams are already adding CRA to RFPs. The question *"is your API gateway CRA-compliant?"* will be standard within 18 months. Traefik answers affirmatively: a European company, a memory-safe codebase, and concrete compliance artifacts ready for customer review.