MONTAVISTA SOFTWARE

Application

# ACHIEVING EU CYBER RESILIENCE ACT READINESS WITH CGX LINUX & MVSECURE

## Introduction: Challenge of EU CRA

As connected devices become more capable, they become more exposed. For manufacturers of embedded systems in telecom, networking, 5G, industrial IoT, medical devices, and other mission-critical markets, cybersecurity is no longer just a technical requirement. It is now a product, lifecycle, and market-access requirement as well.

The **EU's Cyber Resilience Act (CRA)** establishes horizontal cybersecurity requirements for products with digital elements placed on the EU market. The regulation requires manufacturers to address cybersecurity across design, development, production, documentation, vulnerability handling, and post-market support.

For many product teams, the challenge is not understanding the need for security. The challenge is operationalizing it across long-lived Linux platforms that must remain stable, supportable, and certifiable in the field for years.

This application note presents a practical path forward with MontaVista's **CGX Linux** and **MVSecure.** These solutions together give manufacturers a strong foundation for EU CRA readiness by combining a hardened embedded Linux platform, long-term maintenance, vulnerability management, SBOM generation, and security services tailored to mission-critical deployments.

## Understanding EU CRA in Brief

The EU CRA took effect on 10 December 2024. It applies to hardware and software products with digital elements, including operating systems. The framework is built around a few core expectations for manufacturers:

- Perform cybersecurity risk assessment
- Design products to meet essential cybersecurity requirements
- Maintain technical documentation
- Support vulnerability handling throughout the support period
- Carry out conformity assessment
- Provide the information needed for compliant market placement and CE marking

In practical terms, this means embedded product manufacturers need more than a Linux distribution. They need a trusted software base, a disciplined way to monitor and remediate vulnerabilities, visibility into software composition, and a repeatable security process that stands up to internal review, customer scrutiny, and regulatory expectations.

## Why Embedded Linux Teams Need More Than Community Maintenance

Embedded products often remain in service far longer than mainstream software support cycles. A networking appliance, industrial controller, medical platform, or telecom node may need to be maintained for a decade or more. During that time, new vulnerabilities continue to emerge, upstream projects evolve, and compliance expectations tighten.

Trying to manage EU CRA-related obligations with ad hoc patching and community-only maintenance creates risk on multiple fronts. Teams can lose time assessing whether a disclosed CVE is actually relevant, integrating patches without destabilizing fielded systems, and producing the documentation needed to demonstrate due diligence.

MontaVista addresses these pressures by combining a carrier-grade Linux platform with security services designed for long-lifecycle embedded systems.

# CGX Linux: A Secure, Long-Lifecycle Foundation for EU CRA Readiness

CGX Linux is MontaVista's carrier-grade embedded Linux platform, Carrier Grade eXpress, purpose-built for mission-critical, real-time, and long-lifecycle systems. It is designed to deliver RTOS-like performance together with hardened security and more than 10 years of commercial support per release. For manufacturers preparing for the EU CRA, that matters because compliance is not a one-time activity at product launch. It is a lifecycle commitment.

CGX Linux enables support for CRA readiness in several important ways.

First, it provides a hardened, production-ready Linux base. Security is built in through hardened kernel configurations and secure defaults, allowing teams to start from a stronger baseline rather than bolting on protections late in the program.

Second, CGX Linux supports continuous vulnerability monitoring and remediation. MontaVista proactively tracks CVEs, evaluates applicability, and provides tested fixes for the CGX platform. This is especially valuable in embedded environments, where patching cannot come at the cost of uptime, determinism, or reliability. MontaVista's approach is not just to chase vulnerability counts, but to assess which issues matter in the actual deployment context and prioritize accordingly.

Third, CGX Linux supports SBOM generation for compliance and supply-chain transparency. While the EU CRA does not prescribe a single artifact by name as the only acceptable method, it does require manufacturers to understand and document relevant cybersecurity aspects and maintain the technical documentation needed to show conformity. SBOM workflows provide the software composition visibility and traceability needed to support those obligations.

Fourth, CGX Linux is backed by long-term maintenance. Support for 10+ years per release aligns well with the EU CRA's emphasis on vulnerability handling during the support period and helps manufacturers sustain compliance over the operational life of the product.

# MVSecure: Security Services That Turn Platform Capability into Compliance Execution

A strong platform is essential, but regulatory readiness also depends on process, evidence, and execution. MVSecure extends MontaVista's value beyond the operating system by delivering end-to-end Linux security services tailored to embedded systems and evolving regulations like the EU CRA.

MVSecure begins with a security assessment. MontaVista evaluates the customer's system architecture, configurations and controls to identify vulnerabilities and gaps. This directly supports the kind of risk-based approach the EU CRA expects manufacturers to apply before placing products on the market.

From there, MontaVista helps implement system hardening measures such as Secure Boot, SELinux, Linux Integrity Management, Trusted Platform Module (TPM), and related protections. These measures strengthen the trustworthiness of the deployed platform and help reduce exploitable attack surface across embedded devices that are often remotely connected and operationally sensitive.

As importantly, MVSecure includes support for the documentation and certification journey. The EU CRA requires manufacturers to explain in technical documentation how the product complies with the applicable cybersecurity requirements and to complete the relevant conformity assessment steps. MVSecure's security assessment, implementation guidance, and compliance-oriented services allow customers to build that evidence base with more confidence and less internal friction.

## How CGX Linux and MVSecure Work Together for CRA-Oriented Outcomes

The real strength of MontaVista's approach is that CGX Linux and MVSecure are not isolated offerings. Together, they create a practical EU CRA compliance-enablement framework for embedded manufacturers.

CGX Linux supplies the secure and maintainable software foundation: hardened defaults, carrier-grade reliability, long-term support, CVE monitoring, and SBOM capability. MVSecure layers on the expertise and services needed to assess risk, harden configurations, implement security controls, maintain evidence, and align the product lifecycle with evolving regulatory expectations.

This combined model helps customers address CRA-relevant needs:

- **Security by design:** Begin with a hardened Linux platform and strengthen it through structured assessment and implementation.
- **Vulnerability handling:** Continuously monitor, assess, prioritize, and remediate system vulnerabilities over the supported life of the product.
- **Technical documentation and traceability:** Improve software visibility and supporting evidence through SBOM-driven practices and structured security workflows.
- **Operational longevity:** Maintain secure products in the field for the long service lives common in embedded and infrastructure markets.
- **Reduced compliance risk:** Partner with MontaVista for Linux and security expertise to reduce internal effort, accelerate response, and lower lifecycle risk.

## Summary

The EU CRA raises the bar for manufacturers of products with digital elements by requiring cybersecurity to be addressed across the full product lifecycle. The regulation is already in force, with reporting obligations starting on 11 September 2026 and the main obligations applying from 11 December 2027.

MontaVista's answer is a combination of a field-proven Linux platform and comprehensive Linux security services. CGX Linux provides the carrier-grade embedded Linux foundation with hardened security, long-term support, continuous CVE management, and SBOM capabilities. MVSecure extends that foundation with security assessment, hardening, supply-chain security, and compliance-oriented expertise. These solutions allow customers to reduce risk, accelerate remediation, strengthen documentation, and build a path toward CRA readiness for long-lived embedded products.

Please visit www.mvista.com and/or contact us at sales@mvista.com or leave a request for more information on our solutions.

*This application note is informational and should not be treated as legal advice. Manufacturers should assess how the EU CRA applies to their specific products, software supply chains, and market placement model.*


MontaVista Software, LLC, is a leader in embedded Linux commercialization.

For over 20 years, MontaVista has been helping Linux developers get the most out of open source by adding commercial quality, integration, hardware enablement, expert support, and the expert resources of the MontaVista development community. Because MontaVista customers enjoy faster time-to-market, more competitive device functionality, and lower total cost, more devices have been deployed with MontaVista than with any other Linux.

For more information about MontaVista, visit http://www.mvista.com

Media Contact:
MontaVista Software LLC | E: pr-contact@mvista.com | T: +1 (669) 777-6841