Preparing Manufacturers for the EU Cyber Resilience Act

The European Union's Cyber Resilience Act (CRA), passed by the European Parliament in March 2024 and adopted by the EU Council in October 2024, marks a pivotal moment in cybersecurity regulation. This landmark legislation requires all hardware and software products with digital components sold within the EU to meet strict cybersecurity standards by 2027, with various reporting and notification requirements needing to be met by mid-2026.

As the first global regulation to establish mandatory security requirements for product market entry, the CRA addresses gaps in existing EU frameworks and ensures that products are secure throughout their entire lifecycle. For manufacturers, this represents a significant shift, as non-compliance can lead to serious repercussions.

Key CRA Provisions

- **EU-Wide security requirements:** Mandates that products with digital elements, including connected devices and software, meet cybersecurity standards for market access.
- **CE marking:** Products must bear the CE marking, signifying compliance with requirements.
- **Scope:** Applies to products that connect directly or indirectly to other devices or networks, with limited exceptions for products already covered by existing EU cybersecurity rules.
- **Lifecycle security:** Ensures that products are designed, developed, and maintained with cybersecurity in mind, from market entry to post-launch updates and vulnerability management.

Consequences of Non-Compliance

Financial Penalties

Up to €15 million or 2.5% of global annual turnover - whichever is higher - and the potential for additional legal consequences, including lawsuits.

Reputational Damage

Negative publicity, loss of consumer trust, and a weakened market position.

Market Access Restrictions

Non-compliant products can be banned from entering or remaining on the EU market, resulting in loss of revenue and market access.

Meet Compliance Requirements with Finite State

EU CRA Requirements	Finite State Solution
Secure by Design: *All digital products must be developed following a Secure Development Lifecycle to minimize vulnerabilities during production*	Seamless integrations into existing CI/CD pipelines ensuring that source code & compiled binaries are analyzed for security vulnerabilities early in the development process.
Vulnerability Management: *Implement processes to identify, mitigate, & report vulnerabilities within 24 hours to the European Union Agency for Cybersecurity (ENISA)*	Automated, real-time vulnerability detection in source code & binaries across your product portfolio helps identify & assess risks as they emerge. Prioritization features & tailored remediation guidance ensure you find & fix the most critical issues.
Regular Security Updates: *Products must receive security updates throughout their expected lifecycle, with a minimum of five years of support*	Continuous monitoring & alerting ensure ongoing protection & security updates throughout its lifecycle, keeping products compliant with the CRA's minimum five-year support requirement.
Transparency: *Must provide clear & accessible documentation, including software bill of materials (SBOM), user instructions, & security labeling to help consumers make informed choices*	Automated SBOM management generates SBOMs throughout the SDLC, providing comprehensive documentation on third-party components, open-source libraries, & custom code. Easily share & export documents in industry-standard formats (CycloneDX, SPDX)
Conformity Assessments: *Depending on product risk category, self-assessments or third-party evaluations may be required to demonstrate compliance with the CRA's requirements*	Audit-ready reports to demonstrate product compliance, giving you full visibility into your connected product's security. Pen testing for hardware to identify vulnerabilities & weaknesses in physical systems, ensuring their effectiveness in protecting sensitive data & assets.

Contact Us

Learn how Finite State can help your organization meet the CRA's stringent requirements and safeguard your products and business.