RUNSAFE SECURITY

Product Software Security for CRA Readiness

RUNSAFE'S APPROACH TO VULNERABILITY RISK AND LIFECYCLE SECURITY

As products have become increasingly software-driven and connected, vulnerabilities in embedded and third-party software introduce real security risk. Manufacturers' security practices must maintain continuous visibility into all software inside their products, understand vulnerability exposure, and manage cybersecurity risk across the entire product lifecycle. This shift requires more automated processes and tooling to track software, assess risk, and maintain security after a product release. Further, RunSafe protects at runtime against the exploitation of vulnerabilities even when a patch is not applied, dramatically reducing liability exposure.

NEW EUROPEAN UNION REQUIREMENTS

ATo address rising cybersecurity risks in connected devices, the European Union introduced the Cyber Resilience Act (CRA), establishing mandatory security requirements for products sold in the EU market. The regulation applies to products with digital elements — software such as embedded firmware, operating systems, applications, and third-party libraries. Manufacturers are expected to demonstrate:

- Visibility into software components
- Understanding of vulnerability exposure
- Risk-based remediation decisions
- Ongoing security management across the product lifecycle

SOFTWARE TRANSPARENCY

Knowing exactly what software is inside shipped products

- Automated build-time SBOM generation for firmware and software
- Full software inventory across firmware, operating systems, applications, and libraries
- Complete dependency tree visibility including third-party and open-source components

VULNERABILITY & RISK

Understanding which vulnerabilities actually create real risk

- Maps CVEs directly to software components identified in the SBOM
- Determines whether vulnerabilities are exploitable or theoretical risk
- Provides residual risk analysis to guide patch, mitigate, or monitor decisions

HOW RUNSAFE SUPPORTS CRA READINESS

RunSafe helps manufacturers close the operational gaps introduced by the CRA by providing the software visibility, risk clarity, and lifecycle security oversight required to demonstrate secure product development and ongoing vulnerability management.

PRODUCT LIFECYCLE VISIBILITY

Maintaining cybersecurity visibility throughout the product lifecycle

- Continuous SBOM generation tied to product builds to ensure accuracy
- Ongoing vulnerability monitoring against shipped product versions
- Options to make vulnerabilities non-exploitable when patches are delayed or unavailable

A STRONGER CYBERSECURITY POSITION

RunSafe provides technical evidence and reporting that supports these elements.

Component	Supported by RunSafe
Cybersecurity Risk Assessment Report	✓
Secure Development Lifecycle Documentation	✓
Software Bill of Materials (SBOM)	✓
Vulnerability Management & Monitoring Plan	✓
Incident Response & Regulatory Reporting Procedure	✓
Supply Chain Due Diligence Records	✓
Security Update & Support Policy	✓
EU Declaration of Conformity & CE Marking File	✓

*** Subject to RunSafe customers' practice*

WHY RUNSAFE?

RunSafe helps manufacturers provide clear visibility into the software inside their products and understand which vulnerabilities create real risk. By delivering continuous insight into software components, vulnerability exposure, and product lifecycle security, RunSafe enables manufacturers to demonstrate secure product development and maintain the cybersecurity assurance required under the CRA.

ABOUT RUNSAFE SECURITY, INC.

RunSafe Security proactively protects embedded software for both commercial and defense deployments across critical infrastructure, with comprehensive risk identification, protection, and monitoring, ensuring robust, continuous security without affecting performance. Headquartered in McLean, Virginia, with an office in Huntsville, Alabama, RunSafe Security's customers span the aerospace, defense, energy, industrial, and national security verticals. Learn more at: **RunSafeSecurity.com.**