Report

NETRISE

EU Cyber Resilience Act Overview

The EU Cyber Resilience Act (CRA) aims to harmonize cybersecurity standards for products with digital elements across the EU market. This means manufacturers will have a single set of rules to follow when providing products with digital elements to any EU member country.

CRA Cyber Resilience Act

When:

The EU Cyber Resilience Act (CRA) (Regulation (EU) 2024/2847) entered into force on December 10, 2024, following its publication in the Official Journal on November 20, 2024. Key requirements become mandatory in phases, with vulnerability reporting requirements applicable from September 11, 2026 and full enforcement on December 11, 2027. Member States must ensure that conformity assessment bodies (CABs) are available by June 11, 2026 to support manufacturers' pre-market compliance activities.

Enforcement:

Being a regulation, the CRA will be directly applicable in all EU member states. This means that once it comes into effect, it will have the force of law in each country without needing further national legislation to implement it.

Scope:

Non-excluded "products with digital elements" which is defined as "a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately;" (Article 3 'Definitions' (1))

Out of scope are products developed for national security or military purposes, or products specifically designed to process classified information. While it is a general regulation, there are stated exceptions to product categories that are covered under other regulations.

Product Type	Applicable Existing Regulation	Details
Medical Devices	(EU) 2017/745	Clinical investigation and sale of medical devices for human use
IVD	(EU) 2017/746	In vitro diagnostic medical devices
Motor Vehicles	(EU) 2019/2144	Type-approval requirements for motor vehicles and their trailers
Civil Aviation	(EU) 2018/1139	Establishment of a European Aviation Agency to unify standards, including cybersecurity

NetRise Alignment to CRA Essential Cybersecurity Requirements

Annex I of CRA lists the *essential cybersecurity requirements:*

Security Requirements

The following table outlines the requirements outlined in the CRA and the alignment of the NetRise Platform to such requirements. Requirements are broken down into two sections:

Part 1: Cybersecurity requirements relating to the properties of products with digital elements

Clause	Requirement	NetRise
1.	Products with digital elements shall be designed, developed, and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.	NetRise secures the end-to-end lifecycle of software-defined products. During design and development: • Assess supply chain risk during the design stage through ingestion and analysis of third-party SBOMs. Compare SBOMs during development ('SBOMs as designed' to SBOMs post-build 'SBOMs as observed'). • Generate and continuously monitor SBOMs at the product and component levels via analysis of the final production build. Analysis of software prior to the final build cannot guarantee that the CRA requirements are met in production. • Identify and track vulnerabilities across product versions to correlate risk. • Analyze OS security hardening configurations against defined policies and industry best practices. • Identify risks outside of CVEs through analysis of embedded secrets & credentials, cryptographic risk, binary hardening, and more. During production / operational use: • Post-production monitoring for alerting, prioritization, and triage on new vulnerabilities • Bi-directional integrations with CI/CD, ticketing, workflow automation, etc. tools enable a fast feedback loop for vulnerability triage, prioritization, and remediation.

Clause	Requirement	NetRise
2 (a)	Products must be delivered without any known exploitable vulnerabilities.	NetRise identifies known exploited vulnerabilities by deeply inspecting the contents of compiled code, identifying known software components, generating an SBOM, and correlating these known components with CVEs. CVE data is enriched with over 100 sources of advisory and exploit data to identify vulnerabilities: • On the CISA Known Exploited Vulnerabilities (KEV) list • With known weaponized exploits • with known proof-of-concept exploits • Associated with known Threat Actor groups • Associated with Ransomware groups • Associated with botnet activity
2 (b)	Products must be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state.	NetRise's platform confirms secure configurations through a variety of mechanisms: • Identifying known misconfigurations related to standardized industry best practices. • Assessing embedded compiled binaries for binary protection mechanisms (RELRO, PIE, NX, Stack Canaries, etc.). • Detecting default accounts, passwords, SSH keys, and certificates, maintaining an active inventory, and verifying best practices are followed.
2 (c)	Vendors must ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe, enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them.	While the NetRise Platform is not specifically tailored to identify that particular update mechanisms are present and function as intended, NetRise addresses the most difficult portion of this control, which is the identification and continuous monitoring for these vulnerabilities throughout the product lifecycle.

Clause	Requirement	NetRise
2 (d)	Products must ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access.	NetRise assesses systems for vulnerabilities related to unauthorized access in several ways: • Identifying known (i.e. third party) and unknown (0-day) vulnerabilities in binary code that may lead to initial access, privilege escalation, RCE, etc. • Identify hard-coded credentials and other secrets embedded in assessed systems. • Validate certificate/key-based authentication parameters, including encryption strength, as well as alignment to NIST guidelines for Post-Quantum Cryptography (PQC) readiness.
2 (e)	Products must protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state-of-the-art mechanisms, and by using other technical means.	NetRise analysis assesses the maturity and security of the following as it relates to data storage, processing, and transmission best practices/encryption, which are conducive to data confidentiality: • On Linux-based systems (embedded linux for firmware or otherwise), identifying known best practices such as secure directory permissions and additional configuration-related items • Identification of cryptographic material often used for encryption (keys, certificates - for data storage and transmission) and assessing those materials for secure implementation and best practices
2 (f)	Products must protect the integrity of stored, transmitted, or otherwise processed data, personal or other, commands, programs, and configuration against any manipulation or modification not authorised by the user, and report on corruptions.	There are a variety of NetRise capabilities that contribute to identification of risks related to data integrity: • Identification of system misconfigurations that may lead to data integrity loss • From a software supply chain perspective, NetRise's proprietary supply chain knowledge graph allows for not only the identification of vulnerable components (i.e., those with known CVEs), but also potentially risky components based on provenance-related risk (OSS source repository risk such as overall repository health, contributor-related risk, and more - aligned with the OpenSSF scorecard recommendations). • Other aforementioned capabilities such as identification of insecure or default secrets/ credentials, weak cryptographic implementations,

Clause	Requirement	NetRise
2 (f) - con't	Products must protect the integrity of stored, transmitted, or otherwise processed data, personal or other, commands, programs, and configuration against any manipulation or modification not authorised by the user, and report on corruptions.	etc. can uncover risks that may result in data integrity loss. Additionally, NetRise's unique approach to software supply chain security - analyzing the binaries that are built for production (the final product) - allows for cryptographic and other means of verification of build artifacts that are not achievable through traditional DevSecOps practices (e.g. source code analysis).
2 (g)	Products must process only data, personal or other, that are adequate, relevant, and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimization).	Although the analysis that the NetRise Platform provides is not specifically focused on the scope of data that is processed by assessed systems, many of the aforementioned (and below mentioned) capabilities assess systems for risks that may lead to processing of data that is not intended by the system.
2 (h)	Products must protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks.	Essentially all of the NetRise Platform's areas of analysis are designed to identify security-related issues that may lead to lack of availability or downtime: • Identification of known and unknown (0-day) vulnerabilities in compiled code • Misconfigurations • Weak or default credentials, and other embedded secrets • Weak or vulnerable cryptographic implementations • Lack of binary hardening • And more
2 (i)	Products must minimize the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks.	• Essentially all of the NetRise Platform's areas of analysis are designed to identify security-related issues that may lead to lack of availability or downtime for other devices or networks: • Identification of known and unknown (0-day) vulnerabilities in compiled code • Misconfigurations • Weak or default credentials, and other embedded secrets • Weak or vulnerable cryptographic implementations • Lack of binary hardening and more

Clause	Requirement	NetRise
2 (j)	Products must be designed, developed and produced to limit attack surfaces, including external interfaces.	NetRise provides a means of identifying risks that contribute to a larger attack surface in a variety of ways: • Identifying duplicative, out-of-date, and/or vulnerable software components • Identification of high-risk vulnerabilities (such as those on the CISA KEV or with otherwise known exploits) • Identifying and removing unused code (e.g., debug interfaces) that expand the attack surface • Identification of potential 0-days (Common Weaknesses - CWEs) (i.e. Stack Overflow, OS Command Injection, Insecure Function Usage, etc.) • Identification of embedded binaries that lack protection mechanisms • Identification of system misconfigurations • Identification of weak or vulnerable cryptographic implementations
2 (k)	Products must be designed, developed, and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques.	While essentially all of the NetRise Platforms capabilities are specifically designed to reduce the potential for a system to be exploited, the following are highly specific techniques that related to the mitigation of exploitation should an attacker gain unauthorized access to a device or software asset: • Identification of binary hardening mechanisms to prevent further exploitation of compromised systems • Identification of system misconfigurations that could lead to access to protected/sensitive system directories and specific sensitive files • Identification of system misconfigurations that could lead to privilege escalation • Identification of weak cryptographic implementations that could lead to further compromise of sensitive data or privilege escalation • Identification of weak or default credentials that could lead to privilege escalation

Clause	Requirement	NetRise
2 (l)	Products must provide security-related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user.	While the NetRise Platform today does not focus on runtime analysis of data modification / access, an alpha-stage,agent-based product that adheres to this control is scheduled for release in 2026. However, NetRise's current configuration analysis can be customized to identify the presence of functionality that identifies systems in place to conduct such monitoring for CRA compliance reporting.
2 (m)	Products must provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.	While the NetRise Platform does not specifically look for the presence of mechanisms that support the secure deletion or transfer of user data and settings, the current configuration analysis can be customized to identify the presence of such functionality for CRA compliance reporting.

Part 2: Vulnerability Handling Requirements

Clause	Requirement	NetRise
1	Vendors must identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products.	Automates the generation and continuous monitoring of SBOMs for compiled software artifacts (endpoint applications, firmware, containers, mobile applications, and more). Supports the generation and management of both industry standards (CycloneDX and SPDX).
2	Vendors must, in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates.	Provides automated discovery, continuous monitoring, integrated workflow management, actionable guidance, and automated patch validation for a secure software supply chain. NetRise's analysis can be fed back into key developer tools ensuring prioritized risk is surfaced and incorporated into change management.

Clause	Requirement	NetRise
3	Vendors must apply effective and regular tests and reviews of the security of the product with digital elements.	NetRise integrates into CI/CD processes to automatically test all software builds in scope for CRA requirements. In addition to initial tests after build, analyzed software is continuously monitored for emerging vulnerabilities and risk perpetually.
4	Once a security update has been made available, vendors must share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch.	The NetRise Platform supports generation of Vulnerability Exploitability Exchange (VEX) documents, which are specifically designed for vulnerability disclosure in a standardized, machine-readable format.
5	Vendors must put in place and enforce a policy on coordinated vulnerability disclosure.	Industry best practice for vulnerability disclosure recommends the generation and distribution of VEX documents (see control 4 directly above). Enriched vulnerability data within the NetRise Platform can be used to determine impact levels of vulnerabilities, which serve as a key contributor to vulnerability disclosure programs.

Clause	Requirement	NetRise
6	Vendors must take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third-party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements.	See controls 4 & 5 above. Industry best practice for vulnerability disclosure and information sharing recommends the use of standardized VEX documents, which are fully supported by the NetRise Platform.
7	Vendors must provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner.	By creating an inventory of all product-related software, NetRise both analyzes and validates risk mitigation efforts of patching between software versions. This allows Product Security teams to efficiently validate triage and determine which software products are affected by specific vulnerabilities, leading to significantly streamlined processes for distribution of software updates/patches.
8	Vendors must ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.	See controls 4, 5 & 6 above. Industry best practice for vulnerability disclosure and advisories recommends the use of standardized VEX documents, which are fully supported by the NetRise Platform.

Reporting Requirement

From September 11, 2026, manufacturers must notify any actively exploited vulnerability or security incident affecting the integrity, availability, or confidentiality of their products through ENISA's single reporting platform.

The CRA requires manufacturers to submit: an early warning within 24 hours, a detailed notification within 72 hours, and a final report within 14 days of awareness. ENISA's unified platform will serve as a single EU-wide mechanism, connecting to Member State CSIRTs via linked national endpoints.

The NetRise platform supports this requirement by providing flexible reporting formats for vulnerability information exchange, including:

This document last updated October 2025

- **CycloneDX**
- **SPDX**
- **VEX**
- **XLS**
- **API integrations for customization**

About NetRise

Based in Austin, Texas, NetRise protects organizations from cybersecurity risk with a revolutionary approach to software supply chain security. By analyzing compiled code rather than source code, its category-redefining platform creates a software asset inventory that identifies risk within the software actually installed on the systems critical to enterprise infrastructure. With NetRise, software producers and device manufacturers alike build a more accurate view of the software composition of their products. Likewise, cybersecurity professionals within the enterprise and federal government can quickly identify vulnerabilities and other software supply chain risks in the assets that run their organization. NetRise provides both groups with the means to respond quickly to threats identified by the NetRise platform. When unforeseen software vulnerabilities are exploited by bad actors, NetRise enables rapid identification, prioritization, mitigation, and policy updates, reducing material risk to the business. https://www.netrise.io/

NETRISE

What's Inside *Your* Software?

Get a Demo