NETRISE

Data Sheet

NetRise & EU CRA

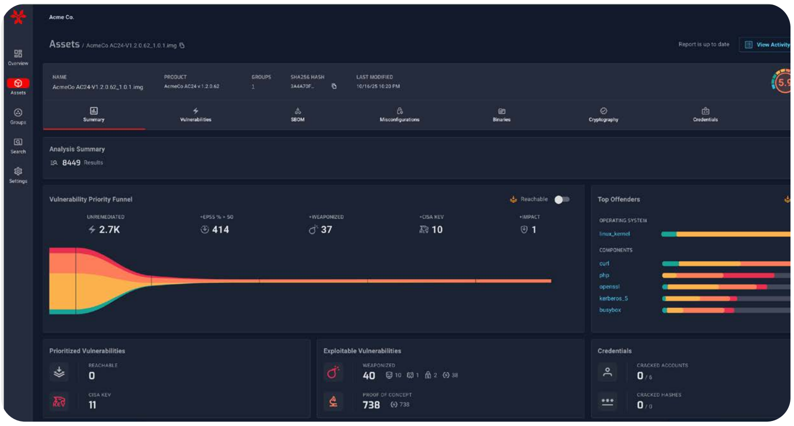
Meet EU CRA obligations by analyzing compiled code, generating SBOMs, and producing audit-ready evidence for regulators.

NetRise provides deep visibility into compiled software running in devices and critical systems, helping organizations meet EU CRA requirements by identifying vulnerabilities, generating compliant SBOMs, and producing audit-ready reports to demonstrate compliance.

What the CRA Demands. What NetRise Delivers.

Requirement Area	CRA Context	What NetRise Provides
Secure software development evidence	Manufacturers must ensure products are secure by design and default, and maintain technical documentation.	Binary-derived SBOMs; visibility into compiled code, configurations, scripts; audit-ready reports.
Vulnerability handling & patch governance	Manufacturers must establish a vulnerability handling process, report actively exploited vulnerabilities to ENISA, and provide timely, secure updates.	Track vulnerabilities and updates; validate fixes; and prioritize remediation by identifying components that load at system startup. Use NetRise's Kernel Vulnerability Auto-Remediation (KVAR) workflow to verify kernel modules, confirm fixes, and cut remediation noise.
Supply chain transparency	Manufacturers must generate, enrich, and validate SBOMs, and capture supply-chain and component relationships.	Generate, enrich, and validate SBOMs for CRA documentation; capture relationships, trace components, and verify third-party data against binary evidence.
Operational prioritization (what actually executes)	Manufacturers must reduce exploitable risks and address high-risk vulnerabilities without delay.	Identify vulnerabilities in components that load at startup to focus remediation on the most exposed code.
Cryptography visibility	Products must apply secure cryptography, manage keys securely, and support modernization per EU standards.	Inventory and validate certificates, keys, and crypto artifacts in binaries and packages.
Reporting & audits	Manufacturers must provide conformity documentation, CE marking evidence, and report vulnerabilities to authorities (e.g., ENISA).	Generate CRA-aligned reports, support ENISA reporting, and demonstrate CE-marking evidence to notified bodies.

Proven Value for CRA Readiness



Acme Co.

Assets / AcmeCo AC24-V1.2.0.62_1.0.1.img

NAME: AcmeCo AC24-V1.2.0.62_1.0.1.img
PRODUCT: AcmeCo AC24 v.1.2.0.62
GROUPS: 1
SHA256 HASH: 3A4A70F...
LAST MODIFIED: 10/16/25 10:20 PM

Analysis Summary: 8449 Results

NetRise gives security and compliance teams faster, clearer insight into what's inside their software. By exposing hidden misconfigurations, hard-coded secrets, and public and private keys, NetRise helps teams reduce risk, verify supplier claims, and generate defensible evidence for regulators and customers.

Binary Analysis

Verify what actually executes in devices and apps without relying on vendor self-assessments or source code.

Audit-Ready CRA Reports

Generate evidence aligned to EU CRA requirements, simplifying conformity documentation and regulator interactions.

Risk Beyond CVEs

Uncover risks from hard-coded secrets, exposed or weak cryptographic keys, and security misconfigurations.

Continuous Supply Chain Insight

Monitor evolving software risks across vendors and assets; verify and validate patches and updates; support ongoing compliance.

Patch Governance & Impact

Track patches and updates, validate fixes, and verify that new versions do not reintroduce vulnerabilities.

Kernel Vulnerability Auto-Remediation (KVAR)

Eliminate kernel vulnerability noise with automated validation and evidence, focusing remediation on exploitable issues—not false positives.

Features & Benefits

Binary Composition Analysis

Find vulnerabilities not found via source-code analysis. Uncover secrets, misconfigurations, and cryptographic keys from beyond what manifests or vendors disclose.

SBOM Generation & Validation

Produce, enrich, and edit SBOMs in SPDX and CycloneDX formats, aligned with CRA lifecycle documentation.

Vulnerability Prioritization

Validate kernel vulnerabilities against actual modules and configurations to focus remediation on truly affected, exploitable components.

Audit-Ready Reporting

Generate EU CRA-aligned reports that map directly to regulator expectations and conformity assessment requirements.

Change History Tracking

Maintain SBOM edits and version history for full lifecycle transparency and regulatory defensibility.

Execution-Aware Analysis

Identify software components that load at system startup to determine which vulnerabilities are actually exposed, enabling defensible reporting within CRA timelines.

Tailored Solutions for Your Role

Build Software

(Manufacturers, OEMs, Developers)

- **Identify and prioritize CVE** and other risks, including secrets, misconfigurations, and unsafe libraries.
- **Generate binary-derived SBOMs** and validate vendor manifests to meet CRA technical documentation and audit requirements.
- **Use kernel vulnerability auto-remediation** to confirm which kernel modules are truly affected before patching.
- **Surface vulnerabilities in startup-loaded components** to focus remediation on the most exposed code.
- **Maintain change history and traceability data** to track component provenance across the software lifecycle.
- **Produce audit-ready reports** aligned to CRA requirements to streamline regulator reviews.

Buy, Use, and Maintain Software

(Enterprises, MSPs, Government, Risk Teams)

- **Verify risk associated with software and devices you buy**, rather than rely on vendor self-attestation.
- **Request CRA-compliant SBOMs and evidence from suppliers**, and use NetRise to validate them during procurement and vendor due-diligence reviews.
- **Monitor vendor patches and confirm vulnerabilities** are remediated across products you operate.
- **Prioritize mitigation based on component exposure** and exploitability, not theoretical CVE lists.
- **Ensure continuous compliance visibility** across purchased devices and embedded software assets.
- **Consolidate CRA and internal audit evidence** for easier compliance reporting and vendor risk management.

What's Inside
Your Software?

Let's Find Out

Who Uses NetRise?

Product Security Engineers
Find risks early, validate SBOMs, and prioritize fixes fast.

GRC & Compliance Teams
Generate audit-ready CRA documentation backed by real binary evidence.

Third-Party Risk Managers
Evaluate supplier software risk and verify CRA compliance evidence.

Firmware Engineers
Uncover vulnerabilities in compiled firmware without requiring source code.

CISOs & Security Leaders
Gain confidence in CRA readiness and software supply-chain transparency.

Procurement Teams
Request and validate CRA-compliant SBOMs and vulnerability evidence from suppliers.

Deploy with Ease

Start Scanning in Minutes
Gain CRA-aligned software visibility almost immediately.

API-First Integrations
Integrate into build pipelines, CMDBs, and risk systems.

Broad OS Support
Analyze Linux, Windows, and RTOS.

Explore Platform Coverage

The NetRise Platform Coverage Sheet provides a detailed look at supported binaries, firmware formats, OS targets, and embedded components—so you know exactly what NetRise can analyze.