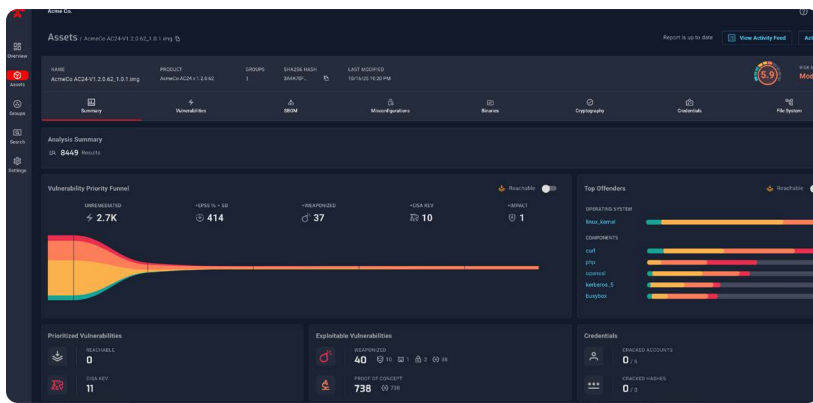


What's Inside Your Software?

Protect your telecom infrastructure from Software Supply Chain Security risk by analyzing compiled code rather than source code.

NetRise provides deep visibility into compiled software across network infrastructure, OSS platforms, 5G core components, edge systems, and customer premises equipment—helping operators identify and manage software supply chain risk to ensure service resilience and compliance.



Why NetRise Is Different

Rather than searching databases and source-derived SBOMs like vulnerability management tools, NetRise analyzes compiled software running on your network devices, finding risk in components beyond what was declared in the source code.

- Prioritize Vulnerabilities That Attackers Have Found:**
 Focus on CVEs that are network accessible, in components that auto-run at startup. Automatically triage and remediate Linux kernels with exploitable paths.
- Non-CVE Risk:** There's more to risk than security flaws in source code. We identify misconfigurations, hard-coded secrets, easily cracked public and private keys, and more.
- Comprehensive and Accurate SBOMs:**
 Why rely on vendor self-attestation when you can verify, then trust? NetRise tells you where you're exposed when incidents occur - without needing access to source code.
- Integrations:**
 NetRise integrates into your workflows and into other tools used in your SOC.



Binary Composition Analysis

Uncover secrets, misconfigurations, and exposed keys across networking, security, and device firmware, plus CVEs in compiled software.



SBOM Management

Generate, enrich, and validate SBOMs for network devices and applications—producing audit-ready evidence aligned with FCC, NIST CSF 2.0, EO 14028, and 5G/6G standards.



NetRise ZeroLens™

Detect exploitable weaknesses in vendor or network software early, before they impact production or customer systems.



Execution-Aware Reachability

Identify which components actually execute, under what conditions and privileges, filtering dormant vulnerabilities to focus remediation on real, exploitable attack surfaces.



Kernel Vulnerability Auto-Remediation

Eliminate kernel vulnerability noise with automated validation and VEX-compliant evidence so teams focus on exploitable issues, not false positives.



Vulnerability Intelligence

Gain deeper context into findings, identifying and prioritizing those that have been weaponized and exploited.

Tailored Solutions for Your Role

For Software Builders

(Telecom OEMs, Equipment Vendors, Software Developers)

- Maintain and publish accurate SBOMs for every version.
- Catch [build-time deviations](#) and unauthorized changes.
- Identify and prioritize CVEs and other risks, including secrets, misconfigurations, and hard-coded secrets.
- Understand reachability and exploitability to prioritize remediation.
- Gain visibility into legacy software components used in core platforms, where source code may be unavailable.
- Demonstrate compliance with regulatory frameworks.

For Those Who Buy, Use, and Maintain Devices

(Telecom Operators, Network Operations, Vendor Risk & Compliance)

- Know what's really executing in your infrastructure.
- Build and maintain a comprehensive software asset inventory.
- Verify risk in vendor devices and software rather than relying on self-attestation.
- Expose hidden risk such as hard-coded secrets, misconfigurations, and public and private keys, which can provide root access across your network.
- Prioritize mitigation based on reachability findings.
- Validate compiled code matches manifests to prevent unexpected components.

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.

What's Inside
Your Software?

Let's Find Out

Who Uses NetRise?

CISOs & CROs:

Gain continuous software supply chain insight for risk and compliance.

Regulatory & Compliance Teams:

Automatically generate binary-derived SBOMs for audits aligned with FCC, NIST, EU CRA, and 3GPP, reducing manual reporting and enhancing regulator confidence.

Third-Party Risk & Vendor Management Teams:

Assess the security posture of network devices and OSS/BSS platforms—no source code required.

Network Operations & SOC Teams:

Identify affected systems and triage vulnerabilities in network devices using exploitability context.

Product & Platform Engineering:

Validate SBOMs, detect risks before deployment, and secure telecom software builds spanning 5G and edge.

Deploy with Ease

NetRise integrates with your existing workflows and reporting tools, streamlining network and device security assessments and compliance processes.



Start Scanning in Minutes

Get visibility into software assets almost immediately.



API-First Design

Integrate into build pipelines, CMDBs, and risk systems.



Cloud-Native

Scale easily without infrastructure overhead.



Broad OS Support

Analyze Linux, Windows, and RTOS.