



# Your Executable Code Hides Risk You Don't Expect

Protect your brand, customer trust, and regulatory standing by verifying that the executable code in your telecom products matches what's documented in your Software Bill of Materials (SBOM).

Illuminate hidden risk in compiled software powering your network equipment, edge platforms, embedded systems, and firmware—exposing vulnerabilities that traditional SBOMs overlook.






SBOM




THE CHALLENGE

# Your SBOM Doesn't Tell the Whole Story

You use the latest application security testing products, and they help your developers write secure code. **But your source-code scanners miss vulnerable components** that your build process inserts into your executables. Without binary composition analysis, this risk remains hidden.

-  Do the component versions in the software build actually match those in your manifest?
-  Have you unintentionally introduced risk through misconfigurations, hard-coded secrets, or public/private keys not seen by AST tools?
-  Can you demonstrate to regulators and telecom customers exactly what's inside the products you provide to your customers?

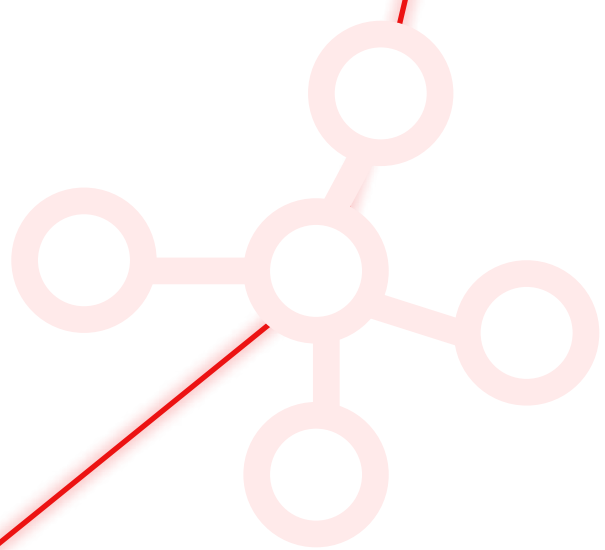
## These gaps persist because:

-  Static testing and SCA don't always reflect what's actually compiled and built.
-  Build processes often introduce old versions of components hidden from SBOMs derived from source code.
-  Legacy tools ignore risk in configuration files, credentials, scripts, and containers.

**For Telecom OEMs, these blind spots create operational, regulatory, and customer trust risks.**



SBOM



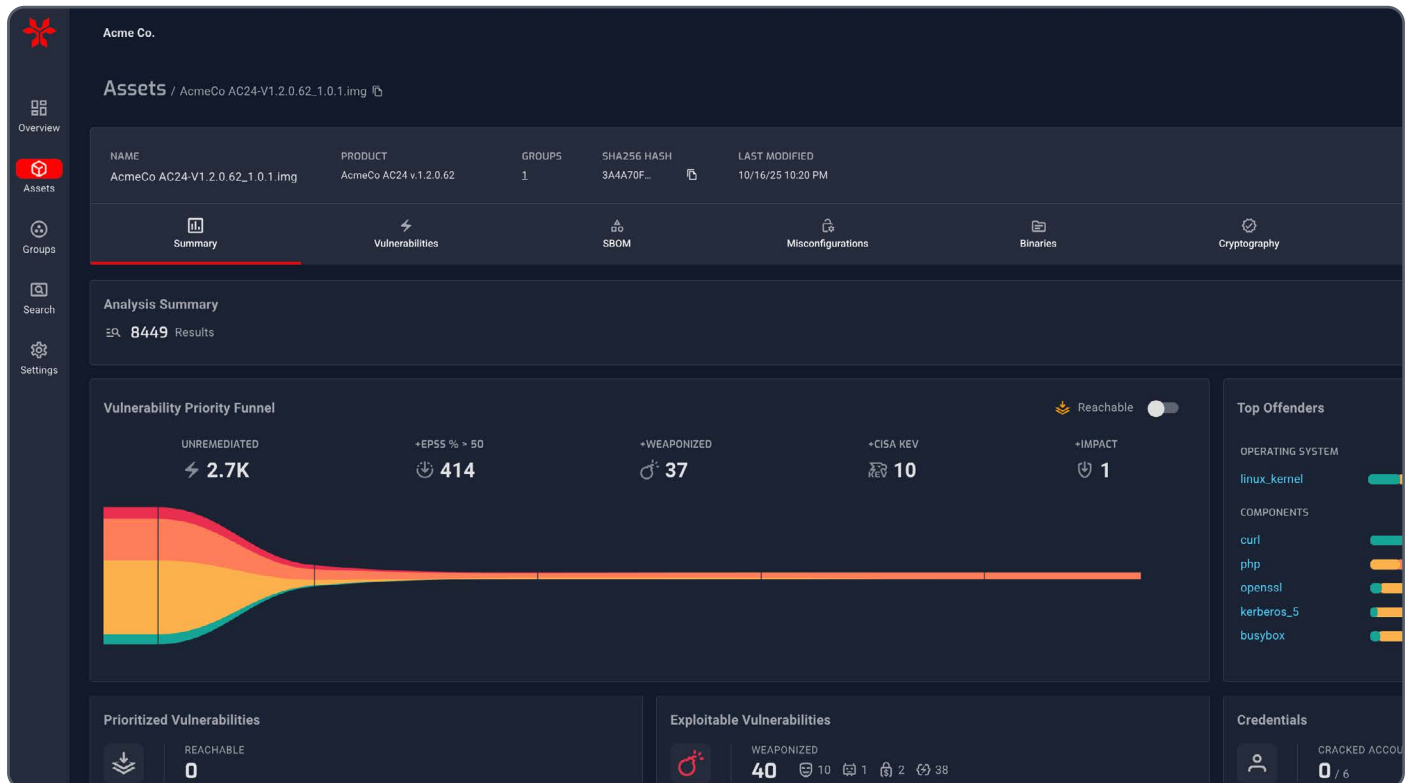
## Why You Need a Comprehensive SBOM

Software today is more assembled than written. Research shows that as much as 80% of today's software is comprised of third-party components. A single application can include proprietary code, open-source libraries, config files, operating systems, credentials, and more.

### THE SOLUTION

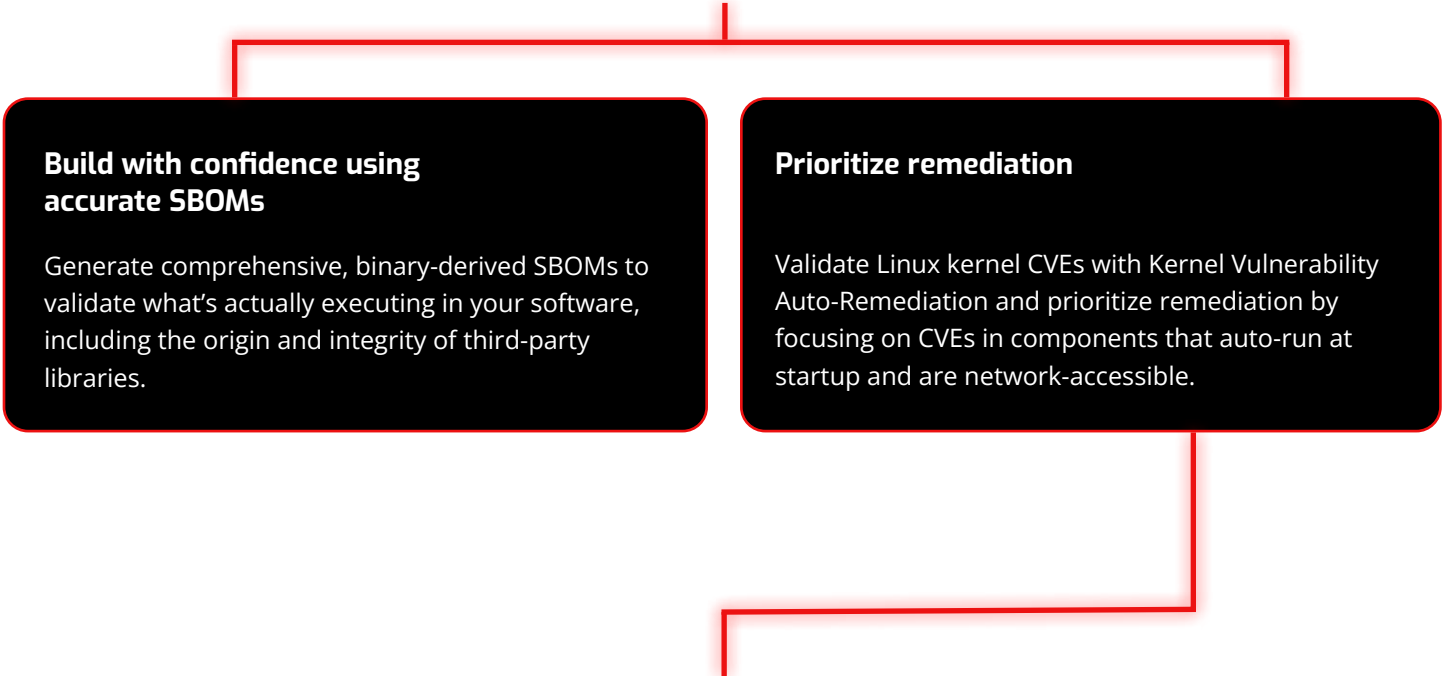
# Software Supply Chain Security for Telecom OEMs

NetRise gives telecom OEMs complete visibility into the software you build—across devices, applications, and vendors—so you can uncover hidden risk, strengthen regulatory defensibility, and make faster, more informed security decisions. Unlike legacy tools limited to source-code analysis, NetRise analyzes the software that actually executes in your products, providing the clarity to prioritize action and reduce exposure.



# NetRise: A System of Intelligence for Telecom Software Security

Whether you build base station software, 5G core components, or customer infrastructure equipment, NetRise helps your teams:




**Build with confidence using accurate SBOMs**

Generate comprehensive, binary-derived SBOMs to validate what’s actually executing in your software, including the origin and integrity of third-party libraries.


**Prioritize remediation**

Validate Linux kernel CVEs with Kernel Vulnerability Auto-Remediation and prioritize remediation by focusing on CVEs in components that auto-run at startup and are network-accessible.


## Platform Overview

 **Binary Composition Analysis**


Analyze compiled software to understand component-level relationships and identify hidden software risk.

 **Compliance Readiness**

Deliver audit-ready evidence for key telecom and cybersecurity regulations—without slowing development.

 **Software Composition Transparency**

Create a binary-derived SBOM offering a comprehensive view of your software supply chain, including source code and other artifacts: misconfigurations, containers, credentials, keys, scripts, and more.

 **Software System of Intelligence**

Leverage enriched context around software vulnerabilities—including a description, a reference to the CVE source, advisories, severity metrics, and more—plus exploitability, reachability, and weaponization status to prioritize real risk in telecom environments.

**NetRise delivers the visibility and context needed to build, certify, and ship secure telecom software and devices.**

# Why NetRise Stands Apart



## Exploit-Aware Prioritization

Focus on real risk with vulnerability intelligence enriched by exploit data, privileges, and CVSS impact.



## Reachability Insights

Identify components that autorun or initialize at startup to prioritize remediation.



## Kernel Vulnerability Auto-Remediation

Eliminate kernel vulnerability noise with automated validation and VEX-compliant evidence so teams can focus on exploitable issues and simplify audits.



## Non-CVE Risk

Surface non-vulnerability risk around misconfigurations, credentials, keys, and licenses.



## Seamless Integrations

Automate workflows across ticketing, compliance, SIEM, and asset management via robust APIs.

## Common Challenges Telecom OEM Developers Face

### Challenge

You struggle to prioritize security findings.

You lack visibility into what's in your compiled builds.

You can't easily see into third-party components.

You need audit-ready documentation.

### How NetRise Helps

**Focus** on vulnerabilities that are weaponized, exploitable, accessible via the network, and autorun at startup.

**Analyze** compiled binaries to validate that the composition of your binaries matches your source code.

**Discover** deeper dependencies than are visible through Software Composition Analysis (SCA) scans.

**Provide** clear, regulator-friendly reports to support telecom cybersecurity compliance.

What's inside *your* software? Build trust and meet customer and regulatory expectations with NetRise.

Get Started