



What's Inside *Your* Software?

Gain visibility into the software running on your network and security infrastructure, OSS platforms, and core and edge systems.

Manage risk in the software your telecom organization buys, uses, and operates.






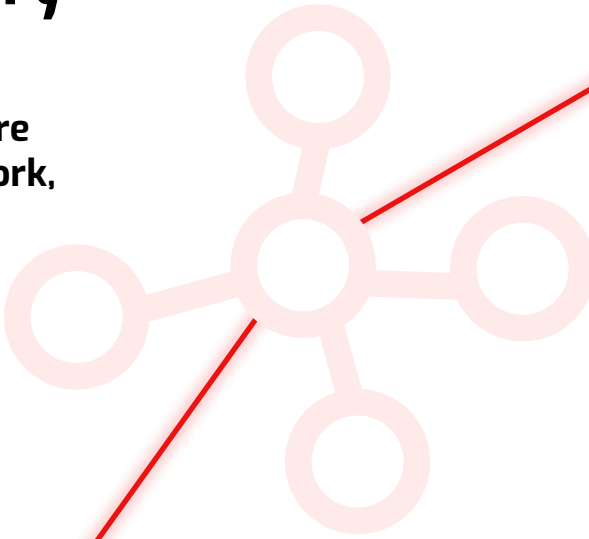
SBOM

THE CHALLENGE




Your SBOM Doesn't Tell the Whole Story

You rely on your vendors' software and firmware to ensure security across your core network, OSS, and edge environments. How do you vet them?

-  Do I have Log4j? If so, where?
-  Does any of my software have malicious contributors?
-  Which devices in my network contain hard-coded or weak credentials?



If you're not sure, you're not alone. Most telecom institutions today rely on opaque software systems into which vulnerability management solutions can't see and third-party risk management tools don't question.

-  Vulnerability management solutions scan devices on your network and rely on publicly available databases to find risk. They don't see what's in the compiled code that executes on those devices.
-  Traditional third-party risk tools and vendor self-attestations provide limited visibility and rely on trust. They don't reveal what's actually inside the software your institution buys and operates.
-  Critical risk lives outside the source code — in containers, misconfigurations, credentials, and hidden scripts.

You maintain full visibility of your network infrastructure. Shouldn't you demand the same for your software?

Where Verification Starts, and Security Follows

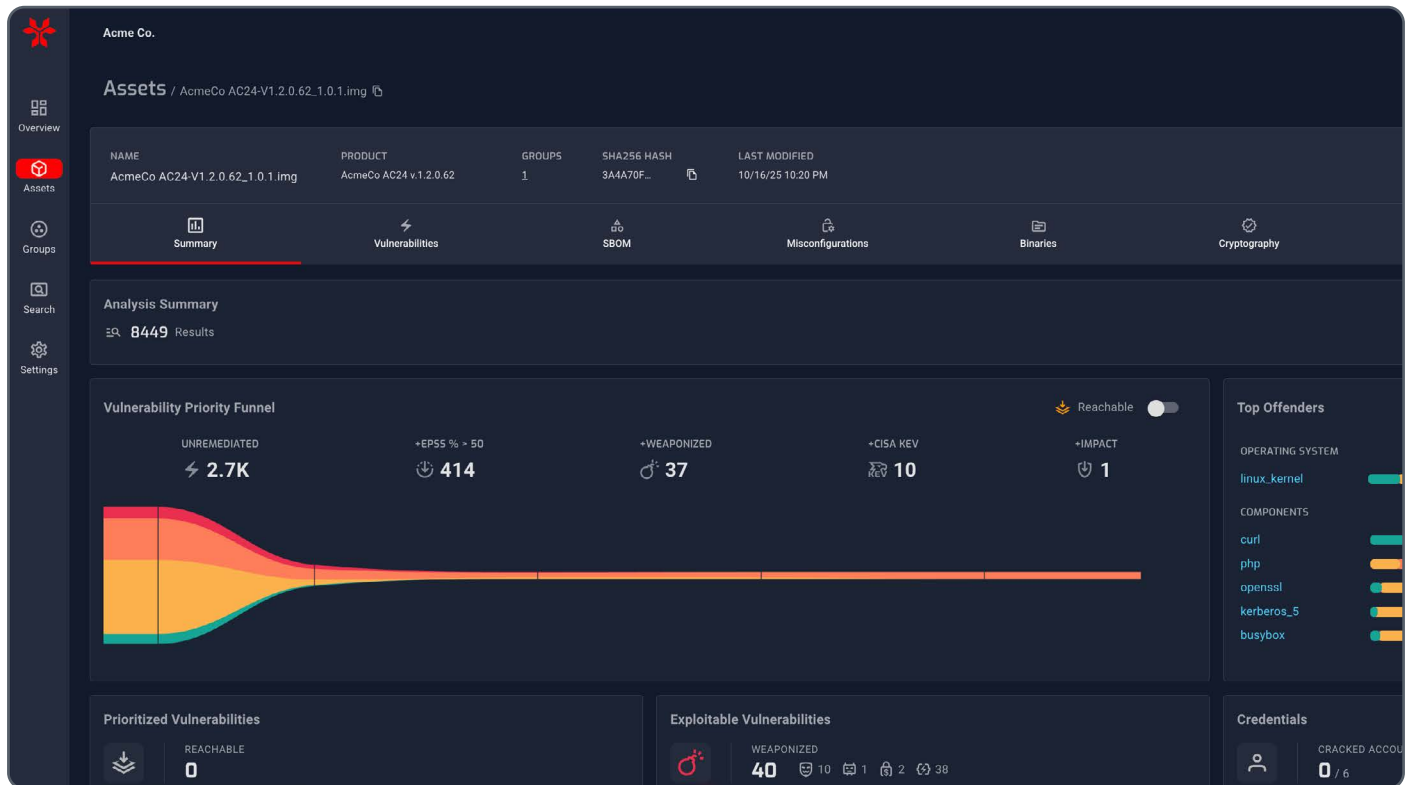
Telecom operators depend on a complex mix of proprietary and third-party code, libraries, dependencies, operating systems, firmware, containers, configuration files, credentials, scripts, virtual machines, and the packages that manage them.

To manage risk, you need visibility into the compiled software actually running in your telecom environment.

THE SOLUTION

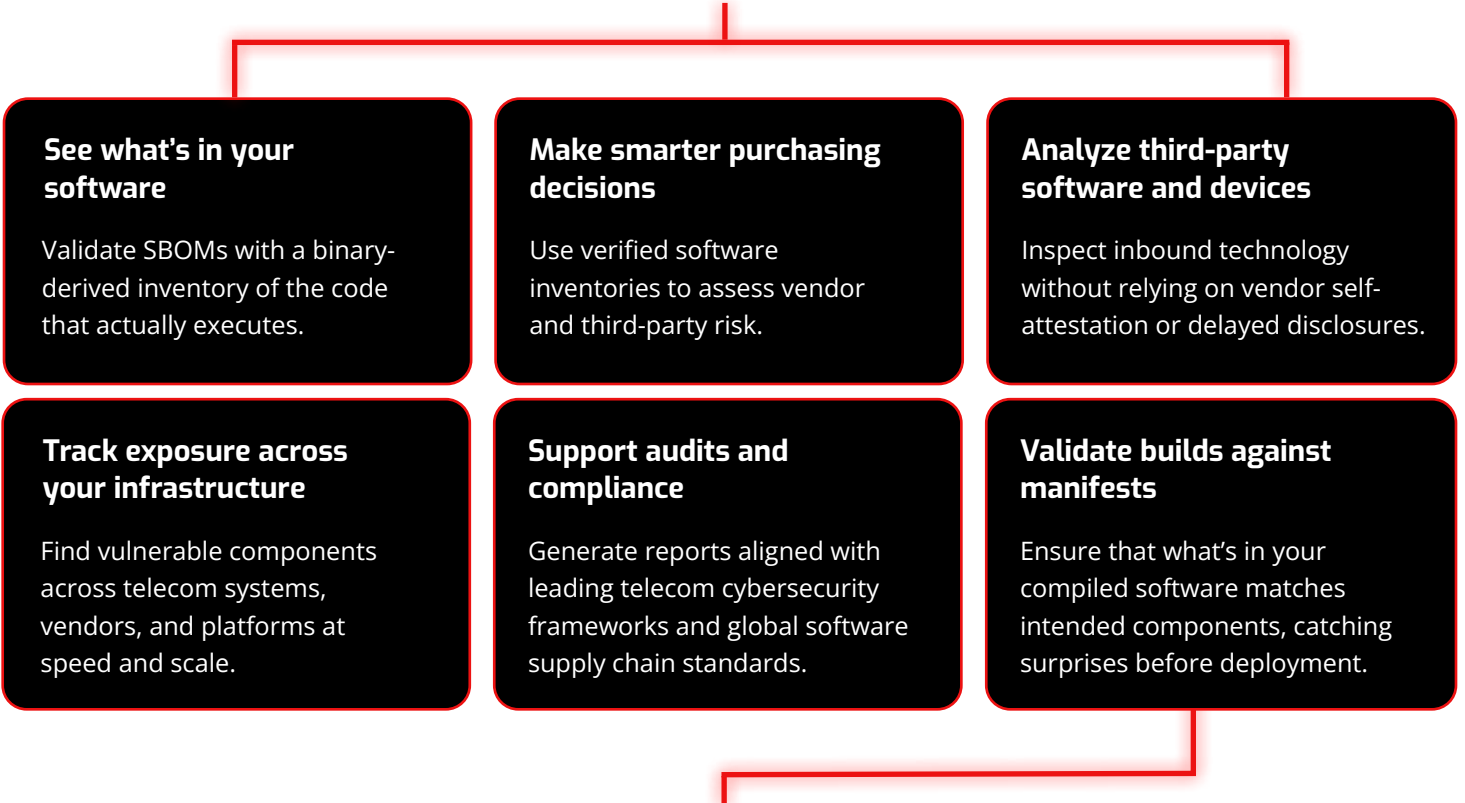
NetRise for Those Who Buy, Use, and Maintain Software

NetRise is redefining software supply chain security for telecom operators. By analyzing compiled code—including firmware in networking devices—NetRise creates comprehensive and accurate software inventories that expose hidden risk, improve security posture, and strengthen regulatory defensibility across core network systems, OSS platforms, edge infrastructure, and CPE.



NetRise: A System of Intelligence for Telecom Network Security

Whether you manage endpoints, deploy third-party software, or oversee critical telecom infrastructure, NetRise helps you:



See what's in your software

Validate SBOMs with a binary-derived inventory of the code that actually executes.

Make smarter purchasing decisions

Use verified software inventories to assess vendor and third-party risk.

Analyze third-party software and devices

Inspect inbound technology without relying on vendor self-attestation or delayed disclosures.

Track exposure across your infrastructure

Find vulnerable components across telecom systems, vendors, and platforms at speed and scale.


Support audits and compliance

Generate reports aligned with leading telecom cybersecurity frameworks and global software supply chain standards.


Validate builds against manifests

Ensure that what's in your compiled software matches intended components, catching surprises before deployment.


Platform Overview

 **Binary Composition Analysis**


No source required. See what actually executes in critical telecom infrastructure, including networking device firmware, containers, and packaged applications.

 **Compliance Without Bottlenecks**

Deliver audit-ready evidence for key telecom and cybersecurity regulations without slowing procurement, onboarding, or operations.

 **Software Composition Transparency**

Build complete, accurate SBOMs that reflect what's truly in your software and devices. Capture additional artifacts such as misconfigurations, credentials, certificates, and scripts.

 **System of Intelligence for Software Risk**

Enrich your software inventory with vulnerability context, CWEs, exploitability, reachability, and licensing indicators to prioritize and manage risk.

NetRise delivers the visibility and context telecom operators need to reduce real-world software risk.

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.

Key Use Cases

Threat Intelligence & Mitigation

Locate, prioritize, and remediate risk fast when new vulnerabilities emerge.

Vulnerability Management

Focus remediation on vulnerabilities that are actually reachable and exploitable, not just listed in an SBOM or CVE feed.

Vendor & Third-Party Risk

Go beyond SBOMs to see what actually executes across networking devices, security appliances, and third-party software—no source code required.

Patch Governance

Validate that patches truly address risk and that updates don't introduce new vulnerabilities or misconfigurations.

Software Asset Inventory

Establish real-time visibility across telecom infrastructure to align with cybersecurity mandates.

With NetRise, you move from software uncertainty to software control.

Get Started