NETRISE

Data Sheet

What's Inside *Your* Software?

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

NetRise provides visibility into the compiled software that runs in devices, apps, operating systems, and in critical infrastructure, so you can prioritize remediation and mitigation of risk to your organization.

Why NetRise Is Different

NetRise assesses the results of a software build, identifying all of the components in the binary image, and finding risk beyond CVEs and CWEs. Our platform tells you which vulnerable code runs at startup, so you can prioritize risk reduction.

- **No Source Code Required:** Rather than rely on vendor self-assessments, verify what runs in the code on devices and in apps you've bought.
- **Beyond CVEs:** There's more to risk than CVEs. We identify misconfigurations, hard-coded secrets, public and private keys, and more.
- **Execution-Aware Reachability**: Identify which components actually execute, under what conditions and privileges, filtering dormant vulnerabilities to focus remediation on real, exploitable attack surfaces.
- **Integrations:** NetRise integrates into your workflows and into other tools used in your SOC.

Binary Composition Analysis

Uncover secrets, misconfigurations, and public and private keys, from compiled software components.

SBOM Management

Generate, enrich, and validate SBOMs for full transparency across all software components.

NetRise ZeroLens™

Identify high-risk CWEs before they are discovered and exploited by bad actors.

NetRise Trace™

AI-powered intent-driven search, based on the underlying motives behind the code.

Kernel Vulnerability Auto-Remediation

Eliminate kernel CVE noise by using configuration intelligence to surface only issues that require action.

Vulnerability Intelligence

Gain deeper context into findings by identifying which vulnerabilities are both accessible via the network and configured to execute at startup.

Open-Source Software Analysis

Analyze open-source dependencies, as well as provenance, contributors, version updates, and more.

Copyright © NetRise Inc. All Rights Reserved.

Tailored Solutions for Your Role

Build Software

(OEMs, Device Manufacturers, Software Developers)

- Maintain and publish accurate SBOMs for every version.
- Catch build-time deviations and unauthorized changes.
- Identify and prioritize CVE and other risks, including secrets, misconfigurations, and unsafe libraries.
- Understand reachability and exploitability with contextual binary analysis.
- Track software lineage, licensing, and provenance across builds.
- Simplify compliance and generate assurance artifacts for customers and regulators.

Buy, Use, and Maintain Software

(Enterprises, MSPs, Government, Third-Party Risk Teams)

- Know what's really executing in your environment.
- Build and maintain a comprehensive software asset inventory.
- Verify risk associated with software and devices you buy, rather than rely on vendor self-attestation.
- Uncover hidden risk due to factors beyond code, such as hard-coded secrets, misconfigurations, public and private keys.
- Prioritize mitigation based on reachability findings.
- Demonstrate compliance with government and industry regulations.

Deploy with Ease

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.

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.

Who Uses NetRise?

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

Third-Party Risk Managers: Assess vendor software and reduce third-party risk exposure.

GRC and Compliance Teams: Generate audit-ready documentation with real software evidence.

Security Operations Teams: Triage vulnerabilities in embedded systems with exploitability context.

Enterprise Software Owners: See what's running, reduce uncertainty, and cut through vendor noise.

Federal Agencies: Achieve EO 14028 and ATO compliance without source code.

What's Inside *Your* Software? Let's Find Out

Copyright © NetRise Inc. All Rights Reserved.