NETRISE

Data Sheet

NetRise for Firmware

Know what is inside shipped firmware, prove it to customers, and respond faster when risk emerges.

NetRise gives teams binary-verified evidence of what is inside firmware by analyzing the full binary image, exposing components and inherited risk that application-layer tools and vendor declarations often miss.

What you get from firmware analysis

Software Builders	Software Buyers
Generate binary-verified SBOMs from the full firmware image to answer questions with evidence.	Verify supplier claims against the full binary image, not application-layer attestations alone.
Catch build-time deviations and unauthorized changes before release to avoid post-shipment surprises.	Build a full-image firmware component inventory to quickly answer where you are exposed.
Find full-image risk beyond the application layer, including secrets, crypto, key-pairs, and misconfigurations.	Triage third-party firmware risk using full-image evidence, not vendor claims that focus on the application layer.
Use provenance policy controls to block, quarantine, or review risky components before release.	Add provenance context to assess component origin, trust signals, and dependency blast radius.
Reduce legal and compliance friction with component- and version-level license visibility.	Reduce time-to-assurance with standards-aligned SBOMs and evidence-ready reporting.

Firmware Artifact Coverage

Embedded Linux firmware families	Android-based, Buildroot, Debian-based, Fedora/Red Hat-based, OpenWRT-based, Windriver Linux, Yocto-based, plus Cisco IOS XE and others
RTOS firmware families	FreeRTOS, Zephyr, VxWorks, ARM RTX, ThreadX/NetX variants, LynxOS, uCOS, and others
Packaging / compression formats	7zip (including self-extracting), ar, bzip2, cpio, gzip, rar, tar, zip, zlib, zstd, xz, and others
File systems and image structures often present in firmware	EXT2/3/4, FAT, GPT/MBR, Initramfs, JFFS/JFFS2, SquashFS variants, UBIFS, YAFFS/YAFFS2, and others

Why NetRise is Different

NetRise gives teams an evidence-based view of what is actually inside firmware and other compiled software by identifying all components in the binary image, not just the application layer traditional VM, IR, TPRM, SCA, SBOM, and questionnaire-based approaches evaluate. NetRise Provenance extends that view by adding source, contributor, organizational, and policy intelligence on top of binary-derived inventory.

- **Beyond the application layer:** See all components in the compiled image, not just the portions traditional VM, IR, TPRM, SCA, SBOM, and questionnaire-based approaches typically evaluate.
- **Risk beyond CVEs:** Surface secrets, misconfigurations, cryptographic exposures, licensing issues, and other non-CVE risk that impacts real-world exposure.
- **Execution-aware context:** Focus remediation on code and components that are reachable, executable, and relevant to the real attack surface.
- **Software trust intelligence:** Add source, contributor and organizational signals, repository health, and policy context so teams can assess trust and blast radius, not just composition.

Deploy with Ease

API-First Design

Integrate into build pipelines, CMDBs, and risk systems.

Start Scanning in Minutes

Get visibility into software assets almost immediately.

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.

Software Asset Inventory

Creates a binary-derived inventory of all components in firmware images, including layers and artifacts application-focused tools do not see.

SBOM Management

Generate, enrich, and validate SBOMs from compiled artifacts for visibility beyond source files, manifests, and application-layer tooling.

Reachability

Prioritize exploitable risk by identifying which vulnerable code is actually reachable via the network and executed.

License Identification

Detect third-party license obligations in compiled firmware to reduce legal exposure and streamline compliance reviews.

Secrets Detection

Expose credentials, keys, and tokens buried in the binary image, beyond what application-layer tools typically uncover.

Provenance

Add source, contributor, organization, blast radius, and policy context to binary-derived inventory for stronger software trust decisions.

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

