NETRISE

Data Sheet

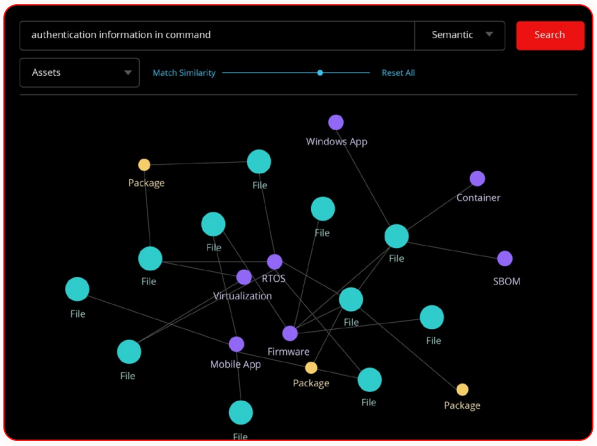
NetRise Trace®

Use intent-driven search to uncover behavioral risk, trace execution paths, and expose inherited vulnerabilities, without source code.

Why You Need NetRise Trace

Traditional scanning stops at known threats. NetRise Trace goes further, into the intent and behavior of compiled code.

Few solutions can uncover dangerous behaviors hidden deep in the software that powers devices and critical systems. NetRise Trace changes that. It enables you to search compiled code by intent, trace behavior across files and languages, and pinpoint the functional blast radius of threats that evade traditional detection.



What NetRise Trace Unlocks

Intent-Based Search

Use natural language or code snippets to surface suspicious behavior.

Blast Radius Mapping

Identify where functions or vulnerabilities appear, and how widely they propagate across packages or builds.

Deterministic Validation

Confirm semantic findings with static analysis and reachability checks tied to CWE and OWASP.

Rescan-Free Querying

Query previously ingested firmware and artifacts without uploading again.

Functional Risk Detection

Use semantic similarity search to interpret the behavior of scripts and configs and surface risky functionality.

Interpreter-Aware Search

Detect risky functionality across multiple scripting languages and interpreters used in software and firmware builds.

Proactive Threat Hunting

Search for anomalies like unauthorized commands or logic inconsistencies before they become exploitable.

Execution-Aware Reachability

Identify which code paths are actually reachable by execution paths at runtime to prioritize exploitable threats.

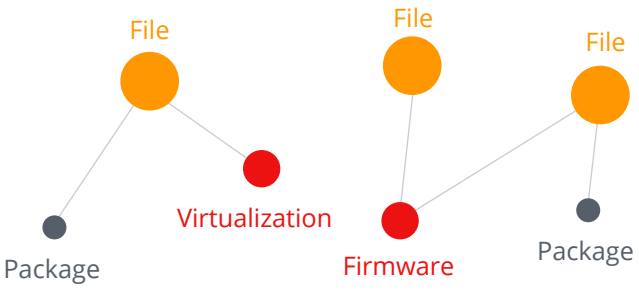
Scalable Behavioral Analysis

Analyze code behavior across broad inventories without sacrificing speed.

Supply Chain Mapping

Visualize how components, packages, and vulnerabilities connect across software and device / asset builds.

How NetRise Trace Works



Trace combines semantic models with a graph-based analysis engine to reveal intent and relationships within your software.

Content Indexed

Shell scripts, Python, firmware, configuration files, container layers, and software images

Behavorial Models

LLM-powered embeddings distinguish dangerous functionality from routine logic

Infrastructure

Built on PostgreSQL with pgvector and BigQuery for scale and search precision

Search Experience

Use natural language or code to generate precise results, including graph visualizations and highlighted matches

Reachability Analysis

Determine which functions or behaviors are executable for runtime-aware prioritization

Who Benefits from NetRise Trace?

Product Security Engineers:
Surface risky command logic early in the development cycle.

Security Operations Teams:
Triage software risk with execution-aware context.

Red Teams and Researchers:
Identify overlooked flaws at scale and link them to reused packages or third-party sources.

Compliance and Risk Leaders:
Validate Software Bill of Materials (SBOM) artifacts and meet audit requirements with artifact-level evidence.

Third-Party Risk Managers:
Independently assess supplier code, trace vulnerabilities, and ensure due diligence.

Incident Response Teams:
Accelerate investigations by quickly identifying risky functionality in affected software, even without source code.

Want to know what your code is doing? Let's trace it.

Request a Demo

Explore behavioral risk in your software supply chain.