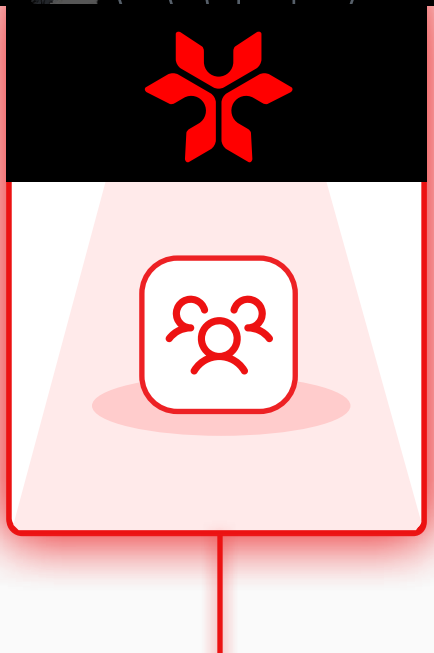
Enterprise Solution Brief

NETRISE

PROVENANCE

Who's Inside Your Software?

80% of your vendor's software is not written by your vendor's employees. See who builds and maintains that open-source software, identify higher-risk contributors or projects, and enforce policies using provenance and repository health signals.

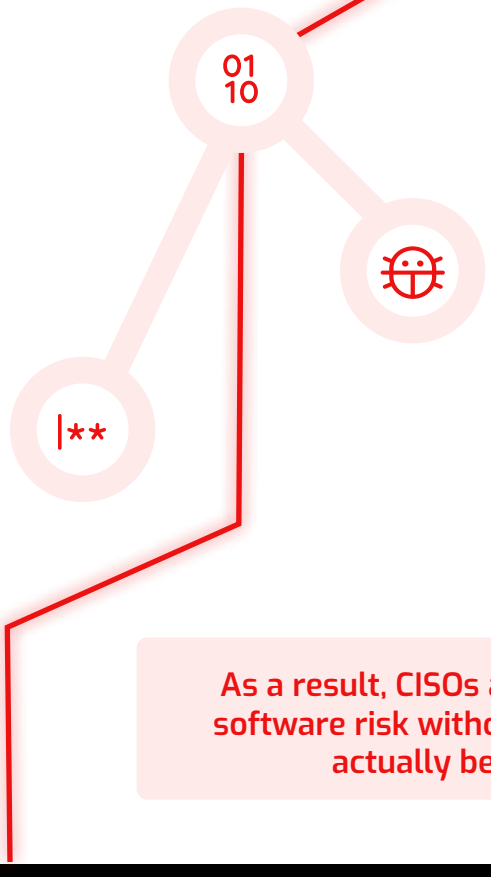


THE CHALLENGE

Can You Trust Software You Can't Verify?

Even with Software Bill of Materials (SBOM) requirements, vendor questionnaires, and security reports, critical questions remain unanswered:

- Do you know who actually writes and maintains the open-source and third-party components inside the software that runs the products you procure?
- Can you identify risk associated with components maintained by malicious contributors, organizations, or countries, or with weak repository health or security practices?
- Are you aware that high-risk individuals contribute to software that's blindly used by vendors, often leading to breaches such as XZ Utils?



These gaps exist because many third-party risk programs rely on incomplete data.

- SBOMs describe what is inside the software, but not who contributes to it nor whether those projects follow basic security practices.
- Vendor disclosures are self-reported and are unaware of how the third-party software they use is built or secured.
- Layers of reused software and code of obscure origin increase the impact when something goes wrong.

As a result, CISOs and risk leaders remain accountable for software risk without a clear, independent view into who is actually behind the software they approve.

Why You Need Provenance Intelligence

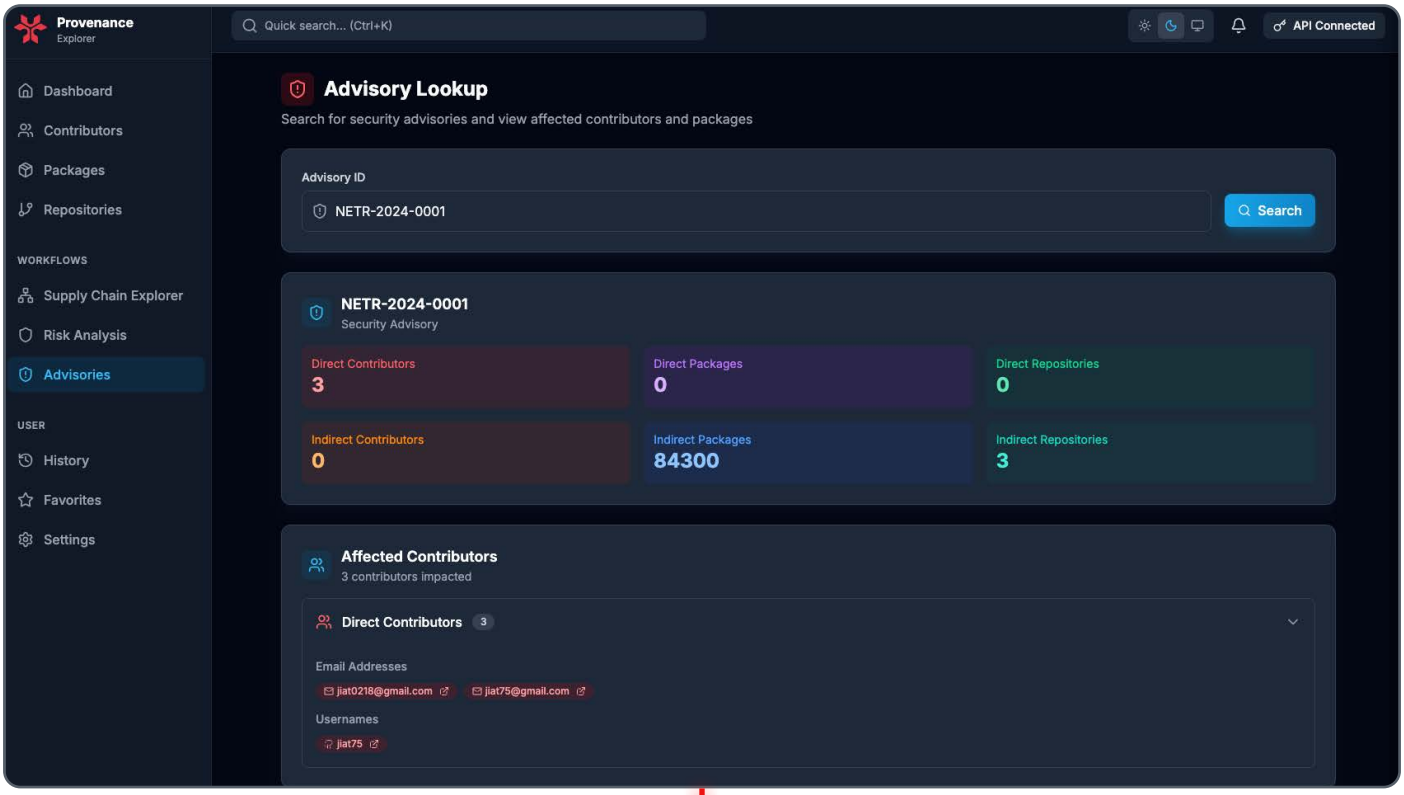
Your vendors increasingly rely on open-source software to deliver their products. They often do not vet that third-party code for risk associated with its contributors.

NetRise Provenance links third-party packages and repos to contributors, organizations, and countries, combining advisories, repository health signals, and risk intelligence to highlight risky third-party software. A built-in policy engine turns these signals into enforceable rules for vendor reviews, onboarding, and renewals.

THE SOLUTION

NetRise Provenance: Trust Intelligence for Enterprise Risk Decisions

NetRise Provenance links components to projects, contributors, organizations, and countries, combining advisories, basic indicators of project security practices, and risk intelligence to highlight risky third-party software so third-party risk reviews, onboarding, and renewals rely on verifiable evidence instead of self-reported claims.



Outcomes for CISOs and Third-Party Risk Teams with NetRise Provenance

Verify the real source of software

Trace components back to their original source projects so you can confirm where the software you buy actually comes from and assess associated risk.

Understand who you are trusting

Open-source software contributors are not your vendors' employees. See the people and locations where software originates to understand how third-party risk is distributed.

Detect high-risk contributors and entities

Use advisories, geolocation, and threat intelligence to flag components linked to known higher-risk contributors, organizations, or countries before they reach your infrastructure.

Make defensible, risk-based decisions

Use repository health and security signals—such as activity, maintainer concentration, update habits, and signing key changes—to support risk-based evaluations of vendor software.

Product Overview

Single Source of Truth

Give CISOs and risk teams one place to see who builds the software you depend on—and enforce consistent software trust policies across vendors.

Maintainer and Organization Attribution

Link software to real people and organizations, including country-level footprint, to support third-party and geographic risk analysis.

Source and Relationship Mapping

Connect software components back to their original projects and see which products from which vendors rely on them, so you can mitigate impact when incidents occur.

Policy-Driven Risk Control

Highlight and enforce rules against higher-risk maintainers, organizations, or projects using advisories, provenance, and repository health signals.

NetRise Provenance delivers the visibility and context your teams need to decide which software and vendors to trust.

Why NetRise Provenance Stands Apart

Built for Enterprise Software Trust

NetRise Provenance is designed for organizations that must make high-impact decisions about software they do not control.

Independent Source of Truth

Identify software origin and contributors to open-source software your vendors use.

Attribution You Can Act On

Understand who maintains critical code and where trust is concentrated.

High-Risk Contributor Detection

Highlight components linked to high-risk maintainers, orgs, or countries using advisories and threat intelligence.

Defensible Risk Evidence

Support audits, regulatory inquiries, and board-level discussions with software-derived proof.

Common Challenges NetRise Provenance Solves

Challenge	How NetRise Helps
Risk associated with open-source software supplied by vendors	Independently links components to original source projects and verifies contributors so you are not relying on blind trust.
Inadequate evidence for third-party risk reviews	Provides contributor, organization, and country information, combined with threat intelligence, to strengthen due diligence.
Difficulty assessing geopolitical risk	Surfaces contributor, organizational, and country-level signals so teams can identify where geopolitical risk concentrates.
Unclear blast radius during supply chain incidents	Shows affected components and products when a risky library, project, or maintainer is identified to prioritize remediation.

Trust software with evidence. NetRise Provenance gives CISOs and third-party risk teams the visibility needed to make confident software procurement decisions.

***Who's* inside your software?** Let's Find Out