RAPIDFORT

SOLUTION BRIEF

# RapidFort Supply Chain Risk Analysis

Independent, deep-binary malware and tampering detection across every image, library, file, and package before it ever reaches your environment.

Software supply chains run components that organizations did not build and cannot fully see. Malicious actors increasingly compromise open-source packages and container layers, embedding threats deep inside artifacts that signature-based scanners and vulnerability lists never reach. Self-reported fixes in new versions are not independently verifiable, and by the time a compromised package is discovered, it is often already running in production.

Security teams need a way to assess every artifact entering their environment images, open-source libraries, files, and packages for malware and tampering before onboarding, not after an incident.

## Solution

Supply Chain Risk mitigation is an integrated profiling and risk assessment capability built into the RapidFort platform. For RapidFort Curated Images (for Red Hat, Ubuntu, Debian, and Alpine) it automatically scans open-source libraries, files, and packages across ecosystems (including npm, PyPI, Maven, and RubyGems) for malware, tampering, and hidden threats, and surfaces the results in a dedicated Supply Chain Risk view.

This assessment is independently powered by ReversingLabs Spectra Assure, giving businesses a security claim backed by an independent, named third-party company rather than a self-reported scan result.

**Up to 99.9%**
CVE elimination in open-source images

**422B+**
files tracked by ReversingLabs threat intelligence

**3-6 Months**
faster time to compliance vs. platform migration

## Key Capabilities

- **Malware-Scanned:** Eliminate malicious binaries and install-time payloads at the source, across images, libraries, files, and packages.
- **Tampering Verification:** Cryptographic and structural analysis helps identify unauthorized modification or repackaging of delivered artifacts.
- **Differential Version Analysis:** Compares new package versions against prior releases to catch newly introduced malware or risky behavior changes.
- **Policy-Driven Release Gates:** Packages that fail security policy are automatically blocked from the catalog until risks are remediated.
- **Evidence-Backed Audit Trail:** Every release includes an independently generated security report for customers, auditors, and regulators.
- **Pin-for-Pin Compatibility:** Drop-in replacement that works with existing OS, tools, and CLI syntax. No migration or proprietary package manager.

## How It Works

### 01

**Assess before inclusion**

Open-source packages from a public repository are automatically scanned for malware, tampering, and hidden threats before they are included, giving security teams a full risk profile.

### 02

**Identify risky updates automatically**

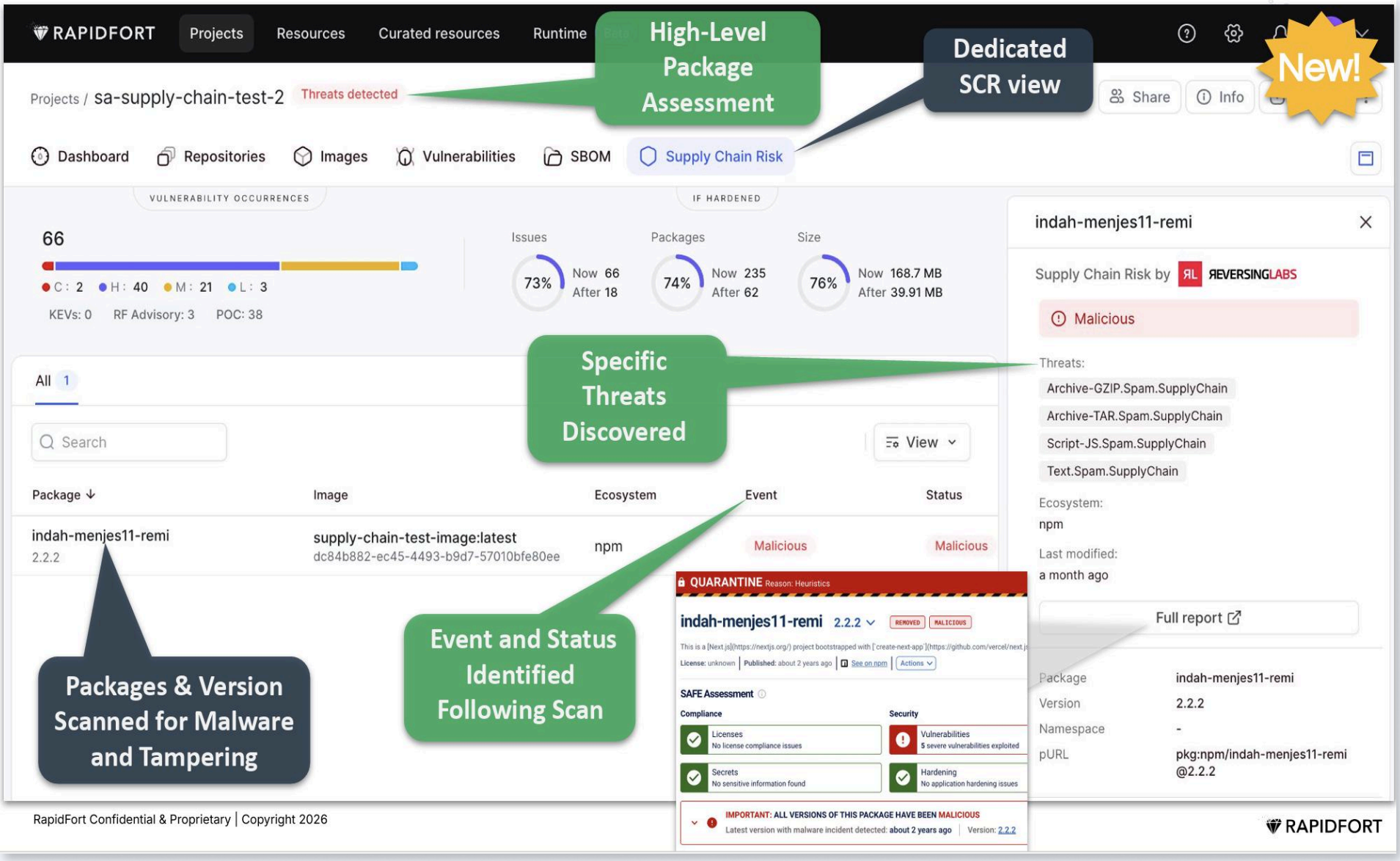
Version-to-version analysis verifies that a new version actually reduces risk instead of introducing a new supply chain risk.

### 03

**Security becomes an enabler, not a bottleneck**

Policy-driven assessments embedded directly in the workflow let teams understand risks to enable rapid decisions.

*RapidFort Supply Chain Risk Analysis*




*Packages are scanned for malware and tampering, with a high-level risk assessment, specific threats identified, and a dedicated Supply Chain Risk view.*

## Why RapidFort

- **Named, independent validation**
  RapidFort is the only vendor whose open-source library catalog is independently validated by a separate, named third-party security company using enterprise-grade deep-binary malware detection.
- **Hardening and risk assessment in one pipeline**
  The RapidFort hardening pipeline has helped enterprise customers eliminate up to 99.9% of CVEs from container images combined with continuous malware and tampering assessment across the same artifacts.
- **No migration, no lock-in**
  Works with standard pip, Maven, npm, and OS package interfaces that teams already use with no proprietary package manager, custom OS distribution, or vendor-specific toolchain required.

## Availability

RapidFort Supply Chain Risk, with open-source library validation powered by ReversingLabs Spectra Assure, is generally available today for Python and Java ecosystems, with JavaScript in closed beta. OS package coverage spans Red Hat, Ubuntu, Debian, and Alpine, with additional language runtimes and application package catalogs on an accelerated roadmap. Existing RapidFort customers can enable Supply Chain Risk and library coverage through the platform console or by contacting their account team.

RAPIDFORT

### About RapidFort

RapidFort leads the Software Supply Chain Security market with the largest distribution of curated, genuinely open-source software, enabling organizations to eliminate risk at scale through hardened near-zero CVE container images, runtime profiling, attack surface management, and independently malware-scanned open-source images. RapidFort is headquartered in Sunnyvale, California.



### Eliminate attack vectors at the source

Schedule a Call ↗

www.rapidfort.com | sales@rapidfort.com