SOLUTION BRIEF · SOFTWARE SUPPLY CHAIN SECURITY

RapidFort Curated Libraries

A comprehensive catalog of malware-scanned and curated libraries

Extends RapidFort protection beyond operating systems, software images, and packages to **independently deployable libraries**.

npm | PyPI | Maven | RubyGems | NuGet

WHERE RAPIDFORT CURATED LIBRARIES FIT

Curated Libraries sit **early in the software delivery process** — before untrusted packages enter the build, artifacts, or production.

Open-Source Ecosystems
npm · PyPI · Maven · RubyGems · NuGet

→

MALWARE-SCANNED · CURATED
RapidFort Curated Libraries
Trusted libraries consumed through existing workflows

→

Build & CI/CD
Build pipelines · packages

→

Images & Artifacts
Container images · internal artifacts

Delivered through **existing package and artifact workflows** — no new security friction — while security teams set policy on approved packages, versions, and images.

The Challenge

- Attackers compromise maintainer accounts, publish malicious updates, or typosquat popular packages.
- Install-time payloads execute before security teams have visibility.
- A discovered package forces reactive investigations: exposure, leaked secrets, and proving compliance.

The RapidFort Solution

- Malware-scanned libraries developers can trust.
- Same versions, interfaces, features, and CLI syntax already in use.
- Consumed earlier in development — a preventive, not reactive, model.

The Result

- Lower likelihood that malware reaches build pipelines, artifacts, or production.
- Prevention up front instead of reaction after public disclosure.

KEY CAPABILITIES

Malware scanning at the source
Helps prevent malicious packages and compromised dependencies from entering pipelines.

Existing workflow support
Works with current operating systems, tools, artifact repositories, interfaces, and CLI syntax.

Reduced incident response burden
Less time hunting for malware and vulnerabilities after public disclosures.

Continuous compliance visibility
Up-to-date assessment and reporting for auditors, customers, and boards.

Policy-driven security
Shift from reactive vulnerability response to a proactive consumption model.

COMMON USE CASES

01 Secure open-source package consumption
Protected libraries for npm, PyPI, Maven, RubyGems, and NuGet ecosystems.

02 Reduce incident-response churn
Limit recurring "are we exposed?" investigations after a newly disclosed malicious package.

03 Protect CI/CD and production environments
Reduce the risk that malware enters a build, artifact, image, or runtime through a dependency.

04 Support audits and customer assurance
Current compliance reporting to demonstrate security controls are in place.

05 Standardize approved software intake
A shared process across engineering and security for consuming open-source libraries, packages, and images.

THREATS ADDRESSED

Helps mitigate supply-chain malware in compromised packages and dependencies, including:

- Malicious binaries
- Backdoored dependencies
- Install-time payloads
- Typosquatted packages
- Credential-stealing code
- Downloaders
- Cryptominers
- Rootkits
- Ransomware

...and other unauthorized changes introduced into open-source components.

BUSINESS OUTCOMES

Developer velocity
Maintain velocity while consuming trusted libraries.

Reduced malware risk
Lower chance of malware entering development and production.

Less incident churn
Less time responding to supply-chain incidents.

Audit-ready posture
Current reporting for customer, auditor, and board-level assurance.

No vendor lock-in
Keep familiar tools and operating systems.

SUMMARY

RapidFort Curated Libraries **shift open-source security from detection and response to prevention** — giving developers malware-scanned, compatible libraries that reduce the risk of compromised dependencies reaching production.

About RapidFort

RapidFort is the leader in Software Supply Chain Security, enabling organizations to eliminate risk across their software stack at scale. Its platform combines curated near-zero CVE container images, runtime profiling, and attack surface management. RapidFort was identified as a Gartner® Cool Vendor™ in 2025 and a Nutanix.Next Partner of the Year in 2026.

up to 99.9%
VULNERABILITIES ELIMINATED WITHIN HOURS

up to 90%
ATTACK SURFACE REDUCED — NO CODE CHANGES