

Software Supply Chain Security for Financial Services

Near-zero CVE minimal images on Linux distributions you already use

RapidFort lets financial institutions run genuine open source while eliminating **up to 99.9%** of security vulnerabilities, with audit-ready evidence and no code changes.

Ubuntu

Debian

Red Hat UBI

Alpine

PyPI

maven

RapidFort covers the full delivery path, from open-source intake through build to production runtime, eliminating inherited risk before and after deployment.

CONTINUOUS END-TO-END SOFTWARE SUPPLY CHAIN SECURITY

INTAKE

Drop-in replacement near-zero CVE minimal images · Brownfield and green field application remediation

BUILD

Signed and malware-scanned RapidFort Libraries (PyPI, npm, RubyGems, maven, etc.)

RUNTIME

Drift detection · Runtime profiling · Continuous compliance dashboard

EVIDENCE

SBOM · RBOM® · Benchmark reports

RapidFort plugs into the registries, package proxies, and CI/CD pipelines you already run, with no code changes, OS changes, or pipeline modifications, and only image metadata leaves your environment.

The challenge

- AI-assisted attackers find and chain open-source vulnerabilities in hours, while change-controlled patching takes weeks.
- Traditional base images ship packages your apps never use, and public registries can carry malicious packages built to look legitimate.
- Examiners and PCI DSS v4.0 expect continuous vulnerability management, but scanner noise and SBOMs that miss what runs leave gaps.

The RapidFort solution

- Curated near-zero CVE minimal images and runtime profiling eliminate CVEs and identify unused code.
- Curated packages block malicious packages and typosquats tampering before they reach your build.
- Your existing pipeline generates SBOM, RBOM®, and benchmark reports automatically.
- Continuous compliance framework with BOD 26-04 standard application fingerprint.

The result

A reference workload dropped from **3,586 applicable CVEs to 3**, with no code changes.

Auditors receive machine-readable evidence of what runs in production.

Key capabilities

01

Curated near-zero CVE minimal images

Minimal images based on Ubuntu, Debian, Red Hat UBI, and Alpine, patched under SLA with version tags preserved.

02

Malware-scanned library intake

PyPI, npm, RubyGems, and maven curated library servers, validated by ReversingLabs, block malicious packages.

03

Runtime-profiled optimizing

Profiler records what executes in an RBOM®, then Optimizer removes unused components to shrink attack surface up to 90%.

04

Risk-based remediation deadlines

Continuous Compliance sets each CVE's deadline from KEV status, exposure, automatability, and impact.

05

Production runtime monitoring

A Helm-deployed Kubernetes agent flags newly disclosed CVEs, tampering, and drift in running workloads.

Common use cases

- | | |
|--|---|
| 01 Simplify internal golden-image work | Large banks can replace duplicated image factories and private forks with one maintained, SLA-patched baseline across lines of business. |
| 02 Scale trading and grid workloads | Curated images pull and scale out faster on Kubernetes and OpenShift; one image shrank from 1.8 GB to 262 MB. |
| 03 Support PCI DSS v4.0 assessments | Payment teams scan cardholder-data environments against PCI DSS v4.0.1 baselines, apply remediation scripts, and hand assessors machine-readable reports. |
| 04 Secure Python intake for quant teams | Asset managers route pip, uv, and Poetry through the Curated Library servers instead of pulling directly from PyPI. |
| 05 Prove production state between exams | Technology risk and audit teams show examiners and auditors RBOM® evidence of what runs in production today. |

Standards supported

RapidFort Continuous Compliance and curated image variants map to the frameworks auditors and assessors use.

CIS Benchmarks

DISA STIG

PCI DSS v4.0.1

NIST 800-171

FIPS 140-3

CISA KEV

CISA SSVC

For EU and UK operations, Runtime aligns with NIS2, EU Cyber Resilience Act, and BSI TR-03183-2 requirements.

Business outcomes

Engineering capacity returned

About 60% less manual remediation effort, returned to delivery work.

No vendor lock-in

Same distros, package managers; exit options preserved.

Fewer examination findings

A smaller vulnerability backlog to defend at each exam.

Audit-ready posture

Evidence stays current between examinations without manual collection.

Lower exploitable exposure

Fewer weaponizable targets in production when new disclosures land.



RapidFort Software Supply Chain Security Platform for Financial Services lets you run the open source your business depends on with near-zero inherited risk, and prove it continuously to auditors and examiners, with no code changes, forks, or lock-in.

About RapidFort

RapidFort leads Software Supply Chain Security with the largest distribution of curated, genuinely open-source software. Its platform combines near-zero CVE minimal container images, runtime profiling, attack surface management, and the first independently malware-scanned open-source images on common Linux distributions. RapidFort appears in the inaugural Gartner® Magic Quadrant™ for Software Supply Chain Security and is a Gartner® Cool Vendor™ and Nutanix .NEXT Partner of the Year.

Up to

99.9%

Vulnerabilities eliminated within hours

Up to

90%

Attack surface reduced, no code changes