RAPIDFORT

KubeCon + CloudNativeCon North America 2026
Salt Lake City · Booth 310 · November 10 to 12

SOFTWARE SUPPLY CHAIN SECURITY FOR KUBERNETES

Eliminate Attack Vectors at the Source

Secure every Kubernetes workload from intake to runtime, on the Linux distributions you already use. Same app. Same distro. Same package managers. A fraction of the CVEs.

Up to 99.9%
of CVEs eliminated, without code changes

Up to 90%
smaller software attack surface

200+
enterprise and public sector customers

RAPIDFORT IMAGES

Change One Line, Not Your Stack

Tens of thousands of minimal, patched, back-ported base and third-party container images, built from source on the Linux distribution you already run, with FIPS and STIG-hardened variants.

DOCKERFILE EXAMPLE

```
- FROM python:3-trixie
+ FROM python:3-trixie-rfcurated
  COPY app.py requirements.txt .
  RUN pip install -r requirements.txt
  EXPOSE 8080
  CMD ["python", "-m", "main"]
```

Measured Reduction

STAGE	IMAGE SIZE	CVES
Original image	1,140 MB	167
Curated base image	250 MB	4
Curated and optimized	89 MB	3

98% fewer CVEs and a **92% smaller** image, with no code changes.

SCANNING AND CONTINUOUS COMPLIANCE

CVE Reachability and Compliance Scanning

Go beyond static SBOM generation and CVE scanning with RapidFort.

CVSS and EPSS Side by Side
Every finding shows CVSS severity alongside EPSS exploit probability, plus patch status.

RF Advisory
CVEs marked not applicable, each with a justification and upstream evidence, to cut scan noise.

Benchmarks and STIGs
Check container images and servers against a wide range of built-in benchmarks and STIGs.

Continuous Compliance
Prioritize your CVE backlog by the CISA BOD 26-04 remediation schedule.

FOUNDING MEMBER
Akrites, a Linux Foundation initiative

SILVER MEMBER
CNCF, listed in the CNCF Landscape

MEMBER
FINOS OSERA, Open Source Enterprise Resiliency Alliance

RECOGNIZED
2026 Gartner® Magic Quadrant™ for Software Supply Chain Security

RAPIDFORT

KubeCon + CloudNativeCon North America 2026
Salt Lake City · Booth 310 · November 10 to 12

RAPIDFORT LIBRARIES

Malware-Scanned Libraries, Drop-In Ready

Drop-in, malware-scanned replacements for the open source libraries you already use, with back-ported patches. A configuration change, not a code change.

Python	JavaScript	Java	Ruby	.NET	Go
PyPI	npm	Maven	RubyGems	NuGet	Go modules

8.7M+

library versions malware-scanned and checked for tampering, without slowing release cycles

- Cooldown on newly published versions
- Threat intelligence from ReversingLabs

Works With Your Tech Stack

Artifact managers	JFrog Artifactory, Cloudsmith, Sonatype Nexus, Google Artifact Registry
Scanners	Trivy, Grype, Twistlock, Snyk, Black Duck, AWS Inspector, Wiz, JFrog Xray

RAPIDFORT RUNTIME

Know What Is Running, What Changed and What to Fix First

Know exactly what is running live in production. Detect what changes. Identify and address new risks before they become incidents.

- One Helm install on any Kubernetes distribution
- Scanner-only or eBPF profiler mode
- No sidecars, no code changes

Continuous CVE Monitoring

Continuously evaluates deployed software against newly disclosed vulnerabilities.

Tamper and Drift Detection

Detects unexpected or unauthorized changes to packages, binaries and processes.

Actionable Mitigation

Practical mitigation recommendations for the security impacts that matter.

Evidence-Based Profiling

Direct evidence of execution reduces false positives and vulnerability noise.

7 of top 10
AI companies are RapidFort customers

3 months
faster FedRAMP for an identity security SaaS provider, with 50% lower hardening cost

2 to 3 weeks
faster major releases reported by customers

VISIT US AT KUBECON

See It Live at Booth 310

Get a live demo of RapidFort Curated Images, Curated Libraries and Runtime.

hub.rapidfort.com

rapidfort.com