RAPIDFORT

DATASHEET

The End-to-End Platform That Eliminates Software Supply Chain Risk

Named in the 2026 Gartner® Magic Quadrant™ for Software Supply Chain Security
Nutanix Global Cloud Native Partner of the Year

Up to 99.9%
CVE Elimination
No code changes. No OS changes. No pipeline modifications.

Up to 90%
Attack Surface Reduction
Shrink your attack surface by removing software you never use.

The Reality of Software Supply Chain Risk

85%
of enterprise software is open source
Most of your risk was written by someone else.

10 hrs
from vulnerability disclosure to active exploit
Down from 24 months a decade ago. Your team still takes weeks.

235,000+
CVEs with known fixes, still unpatched
Across 2016 to 2025. Patching cannot keep pace with the volume.

The industry is solving the wrong problem.

Traditional tools detect and rank vulnerabilities. They do not remove them. Risk stays in your stack indefinitely.
RapidFort eliminates attack vectors at the source, before they reach production.

How it Works

01
Eliminate at the source
Start with RapidFort Images and RapidFort Libraries to remove attack vectors before they enter your software supply chain.

02
Continuously reduce risk
RapidFort Scanner creates an SBOM, identifies and categorizes all vulnerabilities, proposes RapidFort minimal near-zero images, and identifies hardening savings and opportunities.

03
Protect, govern, and prove
RapidFort continuously monitors and protects deployed environments, while RapidFort Continuous Compliance compiles security benchmarks into audit-ready evidence for ATO, NIST, FedRAMP, CMMC, and more.

INTAKE
Eliminate attack vectors ›

BUILD
Scan, analyze, propose ›

RUN
Protect, govern, prove

Platform Capabilities

INTAKE

RapidFort Images

Start with a secure foundation. Near-zero CVEs from day one.

- 50,000+ near-zero CVE images, continuously patched, production-ready, and rebuilt every 24 hours
- FIPS 140-3, STIG, CIS, NIST 800-70 hardened. Drop-in replacements.
- Ubuntu, Debian, Red Hat, Alpine. No vendor lock-in.

INTAKE

RapidFort Libraries

Most supply chain attacks enter through open-source dependencies. Stop them here

- Malware-scanned packages for npm, PyPI, and more
- Pin-for-pin compatible, zero workflow changes required
- Covers the ecosystems most targeted in enterprise and AI workloads

BUILD

RapidFort Scanner

Cut through scanner noise. Know exactly which CVEs actually apply.

- Validates CVE applicability: not just what is installed, but what is real
- Exploit-aware Rapid Risk Score for focused, actionable prioritization
- SBOM export in SPDX, CycloneDX, JSON, and CSV

RUNTIME

RapidFort Runtime

Active real-time monitoring & protection

- Malware/tamper scan results
- CVE discoveries & criticality
- Audit advisory & compliance

RUNTIME

RapidFort Continuous Compliance

Compliance that stays current, not a point-in-time audit.

- US: FedRAMP, CMMC, cATO, DISA STIG, FIPS, NIST 800-53, NIST 800-190, SOC 2, PCI DSS, BOD 26-04
- EU: NIS 2, CRA, SLSA. Validated via the OpenSCAP framework.
- Drift detected immediately. Audit-ready reports and remediation scripts auto-generated.

Why RapidFort

Eliminates, not detects

CVEs are removed from your stack, not added to a backlog.

No code changes. Ever.

Hardening works entirely outside your application code.

Ships faster, stays secure

Cut development costs by over 10%. Speed releases by weeks, not months.

End-to-end, one platform

Intake through runtime. No fragmented tools, no gaps, no blind spots.

Compliance built in

FedRAMP, CMMC, NIS 2, CRA, SOC 2, PCI DSS, FIPS, STIG, CIS.

Government validated

DoD Trusted. Iron Bank Approved. DISA Validated. Mission-critical ready.

RapidFort Vs Everything Else

CAPABILITY	RAPIDFORT PLATFORM	TRADITIONAL ALTERNATIVES
CVE Outcome	✓ Up to 99.9% eliminated. Continuously.	Detected and prioritized. Your team still patches.
Secure Source	✓ 50,000+ near-zero CVE images, ready to drop in	Scanning only. You inherit whatever the base has.
Attack Surface	✓ Up to 90% reduction via intelligent hardening.	Static scanning. Nothing is removed.
Runtime Visibility	✓ Shows what actually executes in production.	SBOM only. No runtime context.
Compliance	✓ FedRAMP, CMMC, NIS 2, CRA, PCI DSS, FIPS, STIG, SLSA.	Point-in-time audits. Manual evidence collection.
Lifecycle	✓ Intake to runtime. One platform. No gaps.	Fragmented tools. Isolated stages.

PROVEN IN PRODUCTION

> *"By leveraging the RapidFort platform, our organization halved our FedRAMP certification costs and reduced time to compliance by a full three months."*
>
> **Borislav Ivanov**
> Director of Engineering, Beyond Identity

FedRAMP · CMMC · cATO · NIS 2 · CRA · PCI DSS · SOC 2 · SLSA · FIPS 140-2/3 · DISA STIG · CIS · NIST 800-53 · NIST 800-190 · DoD Trusted · Iron Bank Approved · DISA Validated

Works with your existing stack:

AWS · Google Cloud · Microsoft Azure · Carahsoft · GitHub · GitLab · Jenkins · Harness · CircleCI · Jira · Splunk · Sumo Logic · Aqua · Prisma · Twistlock · Snyk · Nessus · CrowdStrike

RAPIDFORT

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 minimal container images, aged application libraries, malware removal threat intelligence, runtime profiling, and attack surface management to remove up to 99.9% of vulnerabilities within hours and reduce the attack surface by up to 90% without code changes.

RapidFort, RAPIDFORT, and RBOM® are registered trademarks of RapidFort, Inc.

Eliminate attack vectors at the source

Schedule a Call ↗

www.rapidfort.com | sales@rapidfort.com

440 N Wolfe Rd, Sunnyvale CA 94085