

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 .Next Partner of the Year, 2026

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 Curated Images and RapidFort Curated Libraries to remove attack vectors before they enter your software supply chain.

02 
Continuously reduce risk
RapidFort Analyzer creates an SBOM. RapidFort Profiler generates an RBOM® showing what actually runs. RapidFort Optimizer removes unused components to reduce CVEs and attack surface without code changes







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

INTAKE
Eliminate attack vectors







BUILD
Analyze, profile, optimize

RUNTIME
Protect, govern, prove

Platform Capabilities

 <p>INTAKE</p> <h3>Curated Images</h3> <p>Start with a secure foundation. Near-zero CVEs from day one.</p> <ul style="list-style-type: none"> + 35,000+ near-zero CVE images, continuously patched and production-ready + FIPS 140-2/3, STIG, CIS, NIST 800-70 hardened. Drop-in replacements. + Ubuntu, Debian, Red Hat, Alpine. No vendor lock-in. 	 <p>INTAKE</p> <h3>Curated Libraries</h3> <p>Most supply chain attacks enter through open-source dependencies. Stop them here.</p> <ul style="list-style-type: none"> + 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 	 <p>BUILD</p> <h3>RapidFort Analyzer</h3> <p>Cut through scanner noise. Know exactly which CVEs actually apply.</p> <ul style="list-style-type: none"> + 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
 <p>BUILD</p> <h3>RapidFort Optimizer</h3> <p>Remove every component your application never uses.</p> <ul style="list-style-type: none"> + Up to 99.9% CVE elimination from unused code paths + Up to 90% attack surface reduction via RBOM®-validated hardening + Hardened images automatically rebuilt every 24 hours, drop-in ready 	 <p>RUNTIME</p> <h3>RapidFort Profiler</h3> <p>Your scanner sees what is installed. Profiler sees what actually runs.</p> <ul style="list-style-type: none"> + Generates RBOM®, RapidFort's proprietary Runtime Bill of Materials + Separates real exploitable risk from theoretical CVE noise + Under 1% overhead. No code changes. No disruption. 	 <p>RUNTIME</p> <h3>RapidFort CART</h3> <p>Compliance that stays current, not a point-in-time audit.</p> <ul style="list-style-type: none"> + US: FedRAMP, CMMC, cATO, DISA STIG, FIPS, NIST 800-53, NIST 800-190, SOC 2, PCI DSS + EU: NIS 2, CRA, SLSA. Validated via the OpenSCAP framework. + Drift detected immediately. Audit-ready reports and remediation scripts auto-generated.

Why RapidFort

 <h3>Eliminates, not detects</h3> <p>CVEs are removed from your stack, not added to a backlog.</p>	 <h3>No code changes. Ever.</h3> <p>Hardening works entirely outside your application code.</p>	 <h3>Ships faster, stays secure</h3> <p>Cut development costs by over 10%. Speed releases by weeks, not months.</p>
 <h3>End-to-end, one platform</h3> <p>Intake through runtime. No fragmented tools, no gaps, no blind spots.</p>	 <h3>Compliance built in</h3> <p>FedRAMP, CMMC, NIS 2, CRA, SOC 2, PCI DSS, FIPS, STIG, CIS.</p>	 <h3>Government validated</h3> <p>DoD Trusted. Iron Bank Approved. DISA Validated. Mission-critical ready.</p>

RapidFort Vs Everything Else

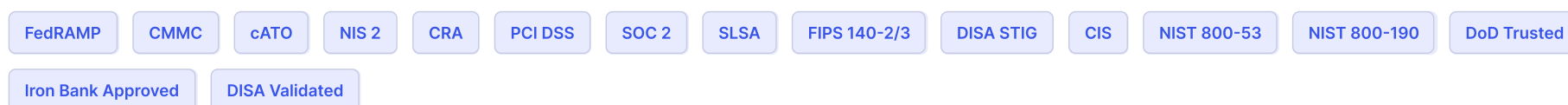
CAPABILITY	RAPIDFORT PLATFORM	TRADITIONAL ALTERNATIVES
CVE Outcome	🟢 Up to 99.9% eliminated. Continuously.	Detected and prioritized. Your team still patches.
Secure Source	🟢 35,000+ near-zero CVE images, ready to drop in.	Scanning only. You inherit whatever the base has.
Attack Surface	🟢 Up to 90% reduction via RBOM®-validated hardening.	Static scanning. Nothing is removed.
Runtime Visibility	🟢 RBOM® 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

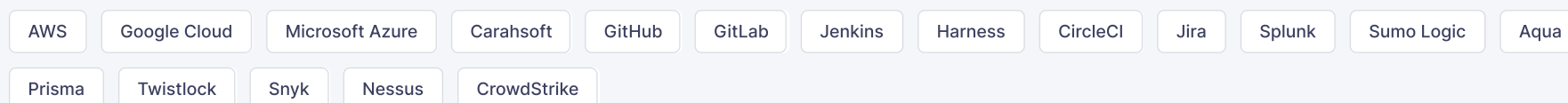
“By leveraging the RapidFort platform, our organization halved our FedRAMP certification costs and reduced time to compliance by a full three months.”

Borislav Ivanov

Director of Engineering, Beyond Identity



Works with your existing stack:



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, 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