RAPIDFORT

WHITEPAPER

Secure Software Development Lifecycle

The RapidFort approach to eliminating vulnerabilities at every stage of the SDLC.

SECURE SDLC | RISK REDUCTION | NEAR-ZERO CVE IMAGES



© 2026 RapidFort, Inc. | www.rapidfort.com

01 EXECUTIVE SUMMARY

Understanding the Traditional SDLC Challenges

The escalating frequency and severity of cyberattacks underscore the critical need for a strong security posture throughout the software development lifecycle (SDLC). Security has traditionally been treated as an afterthought, which contributes to costly breaches. This white paper explains how RapidFort's approach transforms the SDLC, eliminating Common Vulnerabilities and Exposures (CVEs) at every stage to deliver resilient, secure software.

85%

of enterprise software is open source

10 hrs

from vulnerability disclosure to active exploit

235,000+

CVEs with known fixes identified, 2016 to 2025

02 THE CHALLENGE

The CI/CD Security Challenge

The traditional SDLC often prioritizes speed and functionality over security, creating conditions that are easier for attackers to exploit. Key challenges include:

- **Late-stage security testing:** Identifying vulnerabilities after development is costly, time-consuming, and often requires significant code refactoring.
- **Insufficient developer security awareness:** Many developers lack in-depth security expertise, which can lead to unintentional vulnerabilities and insecure misconfigurations.
- **A complex and evolving threat landscape:** The changing nature of threats demands continuous adaptation and mitigation. In addition, AI has accelerated the uncovering of CVEs and sped up the time from discovery to exploit.
- **Compliance mandates:** Adhering to frameworks such as FedRAMP, NIST, and SOC 2 while maintaining development velocity is a difficult balance.
- **DevOps integration challenges:** Building security into high-velocity DevOps pipelines requires the right tools and processes.

RapidFort's approach to a secure SDLC

RapidFort addresses these challenges by eliminating risk at the source and continuously reducing the attack surface across the full software lifecycle, spanning intake, build, and runtime.

INTAKE

RapidFort Curated Images

RapidFort Curated Images, hardened to NIST 800-70 and FIPS 140-2/140-3 validated, refreshed continuously

BUILD

RapidFort Analyzer and Optimizer

RapidFort Analyzer and Optimizer generate an SBOM and continuously harden the build to reduce the attack surface

RUN

RapidFort Profiler and Continuous Compliance

RapidFort Profiler and Continuous Compliance generate the Runtime Bill of Materials (RBOM®) and compile audit-ready compliance evidence

STEP 1 - INTAKE

Building a Secure Foundation with Near-Zero CVE Images

A strong foundation is essential for secure software development. RapidFort Images provide that starting point by eliminating known vulnerabilities from the outset.

- **A broad image library:** Tens of thousands of near-zero CVE images across Ubuntu, Debian, Red Hat, and Alpine.
- **Continuously patched:** Images are refreshed continuously to stay ahead of newly disclosed vulnerabilities.
- **A hardened foundation:** FIPS 140-3 validated images, PQC-ready images, hardened to NIST 800-70 and benchmarked to STIG and CIS.
- **Compliance alignment:** Images are built to align with major compliance frameworks, reducing the compliance burden on development teams.

By building on RapidFort Images, organizations can meaningfully reduce their attack surface, accelerate development timelines, and demonstrate a strong commitment to security from the very first line of infrastructure.

STEP 2 - BUILD

Reducing Risk with Deep Analysis and Continuous Hardening

Early identification of vulnerabilities and continuous removal of unused components are essential to preventing security incidents before they occur. RapidFort Analyzer and Optimizer give teams visibility into real risk while continuously reducing the attack surface during the build stage.

- **Accurate analysis:** RapidFort Analyzer generates an SBOM and validates which CVEs are actually applicable.
- **Continuous hardening and optimization:** RapidFort Optimizer removes unused components to reduce both attack surface and image size.
- **Seamless workflow integration:** Vulnerability detection and hardening integrate directly into existing CI/CD pipelines with minimal disruption to developer workflows.
- **Integrated benchmarking:** CIS and STIG benchmarks are built directly into the analysis and hardening workflow.

STEP 3 - RUNTIME

Continuous Visibility and Compliance at Runtime

Maintaining a secure posture requires ongoing visibility into what actually runs in production. RapidFort Profiler and CART keep applications protected and audit-ready well after deployment.

- **Runtime visibility:** RapidFort Profiler generates RBOM®, RapidFort's Runtime Bill of Materials, showing what actually executes rather than just what is installed.
- **Reduced noise:** By separating real, exploitable risk from theoretical CVE noise, teams spend less time chasing vulnerabilities that do not apply to their running workloads.
- **Compliance enforcement:** RapidFort CART continuously monitors adherence to industry regulations and standards and compiles audit-ready reports and elimination guidance.
- **Risk-based vulnerability management:** Vulnerabilities are prioritized based on real risk and impact, supporting more efficient elimination and patch management.

RapidFort's continuous monitoring capabilities help organizations stay ahead of emerging threats and demonstrate a proactive security posture across every deployment.

03 CONCLUSION

A Secure SDLC, from Intake to Runtime

By integrating RapidFort into the SDLC, organizations can meaningfully strengthen their software security posture, reduce risk, and support broader business objectives. This approach builds a culture of security, giving development teams the confidence to build and deploy software without trading away speed. Taking a proactive, comprehensive approach to security helps organizations protect their brand reputation and stay ahead of an evolving threat landscape.

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 hardened near-zero CVE container images, 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 appears in the inaugural Gartner® Magic Quadrant™ for Software Supply Chain Security and is a Gartner® Cool Vendor™ and Nutanix Global Cloud Native Partner of the Year.

© 2026 RapidFort, Inc.

Eliminate attack vectors at the source

Schedule a Call ↗

www.rapidfort.com | sales@rapidfort.com