RAPIDFORT

WHITEPAPER

Accelerating Secure Software Delivery with a Three-Step Approach

How RapidFort helps organizations eliminate vulnerabilities at the source across cloud-native environments.

CLOUD-NATIVE ERA | 3-STEP APPROACH | SECURE SOFTWARE DELIVERY



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

01 Executive Summary

Security for the Cloud-Native Era

The rapid evolution of cloud-native architectures has brought organizations unprecedented agility and scalability. That same transformation has also introduced a complex set of security challenges. The distributed nature of microservices, the accelerating pace of software development, and an intricate software supply chain create conditions where vulnerabilities can be exploited. Addressing these risks and protecting the integrity of cloud-native applications requires a comprehensive, proactive approach to security.

RapidFort addresses these challenges through a three-step approach to secure software delivery. By building on curated and hardened, near-zero CVE base images, continuously analyzing and profiling applications, and optimizing workloads at runtime, organizations can meaningfully reduce their attack surface, strengthen compliance, and accelerate time to market.

Up to 99.9%
of vulnerabilities eliminated within hours

Up to 90%
reduction in software attack surface

Tens of thousands
of near-zero CVE curated images

This white paper explores the security challenges facing cloud-native organizations, walks through RapidFort's three-step approach, and looks at how large organizations in particular can use the platform to streamline DevOps and strengthen their security posture.

02 The Challenge

The Evolving Threat Landscape

The cloud-native paradigm has fundamentally changed how software is developed, deployed, and managed. Alongside its benefits, it has introduced a new set of security challenges:

- **A complex attack surface:** The distributed nature of microservices creates a large, intricate attack surface that is difficult to fully identify and protect.
- **Supply chain risk:** Reliance on third-party components and open source software introduces vulnerabilities that can propagate throughout an application ecosystem.
- **Rapid development cycles:** The accelerated pace of development can cause security to be deprioritized in favor of speed, increasing the risk of vulnerabilities being introduced.
- **Dynamic environments:** Cloud-native applications run in highly dynamic environments, making it difficult to maintain consistent security controls.

Addressing these challenges effectively requires a holistic approach that spans the entire software development lifecycle, from intake through build to runtime.

03 The RapidFort Approach

RapidFort's Three-Step Approach to Secure Software Delivery

RapidFort offers a proven approach to securing cloud-native applications, spanning three key steps.

STEP 1 · INTAKE

Build on a Solid Foundation

- RapidFort Images, hardened to NIST 800-70
- FIPS 140-3 validated and PQC-ready images
- Justification support for Plan of Action and Milestones (POA&Ms)
- Continuously refreshed images

STEP 2 · BUILD

Gain Deep Visibility and Control

- RapidFort Analyzer generates an SBOM
- RapidFort Optimizer identifies and can remove unused components
- Up to 90% reduction in software attack surface
- Integrated CIS and STIG benchmarks

STEP 3 · RUN

Monitor and Stay Compliant

- Generates the Runtime Bill of Materials (RBOM®)
- Prioritizes vulnerabilities by real exploitability
- Under 1% overhead
- Compiles audit-ready compliance evidence

Step 1: Build on a solid foundation

The cornerstone of secure software development is a trusted foundation. RapidFort Images serve as the starting point for application development. These images are hardened and continuously refreshed, eliminating common vulnerabilities and reducing the attack surface from the outset. By building on these curated and hardened images, organizations can accelerate development while maintaining a stronger security posture.

Step 2: Gain deep visibility and control

Understanding the composition and dependencies of an application is essential for effective vulnerability management. RapidFort Analyzer generates a detailed SBOM, while RapidFort Optimizer can continuously remove unused components to reduce the attack surface. Together, these tools help organizations identify

Step 3: Gain deep visibility and control

Continuous visibility and monitoring are essential to maintaining a secure application environment. RapidFort Profiler continuously tracks what actually executes in production, generating RBOM® to separate real, exploitable risk from theoretical CVE noise. RapidFort integrates directly with CI/CD pipelines, so security is embedded into the development process rather than bolted on afterward, and RapidFort Continuous Compliance supports ongoing monitoring to help teams stay ahead of emerging risk.

DevOps teams are under constant pressure to deliver software faster while maintaining high quality. Manually patching vulnerabilities is time-consuming and prone to error. RapidFort continuously eliminates vulnerabilities, freeing DevOps teams to focus on delivering new features and improving application performance.

By taking a preventative rather than reactive approach to security, organizations can meaningfully reduce the risk of breaches and limit the impact of incidents. RapidFort Platform helps DevOps teams build and maintain secure software without trading away speed or agility.

04 Enterprise Scale

Accelerating Secure Software Delivery for Large Organizations

Large organizations face distinct challenges in securing complex IT environments. Meeting demanding regulatory requirements, protecting sensitive data, and coordinating across multiple development teams calls for a security approach that can scale.

Centralized visibility

Gain insight into the security posture across an entire application portfolio.

Scalability

Support growing workloads and increasing application complexity as the organization scales.

Compliance support

Build toward major industry frameworks, including FedRAMP, NIST, FIPS, STIG, CIS, SOC 2, and PCI DSS.

Integration capabilities

Integrate with existing security tools and infrastructure already in use across the organization.

By adopting RapidFort, large organizations can streamline their security operations and manage risk more effectively across a growing application portfolio.

05 Conclusion

Secure Software Delivery, Built for the Cloud-Native Era

Securing cloud-native applications is no longer optional. RapidFort offers a comprehensive approach to address the challenges facing organizations of every size. By combining curated and hardened images, deep visibility, and continuous optimization, RapidFort helps organizations accelerate secure software delivery while maintaining a strong security posture from intake through runtime.

To learn more about how RapidFort can support your organization's security goals, visit rapidfort.com or reach out to our team.

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