

WHITE PAPER



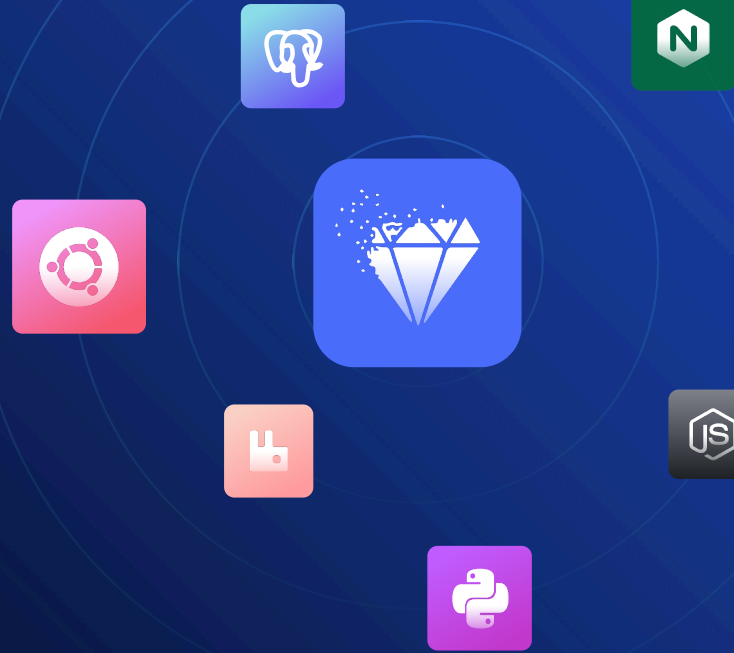
Get to Near-Zero CVEs with no code changes

# RapidFort SASM Platform

Curated Container images, Profiling, & Hardening tools

# Executive Summary

The rapid pace of software development, fueled by CI/CD pipelines, can introduce security vulnerabilities. This white paper explores the key challenges in balancing speed with security within the CI/CD pipeline. It introduces RapidFort as a comprehensive solution that seamlessly integrates scanning tools, curated container images, and Software Attack Surface Management (SASM) capabilities within your CI/CD workflow. We'll highlight how RapidFort's automatic scanning and hardening of containers can remediate up to 95% of software vulnerabilities, significantly reducing your attack surface and streamlining development. Additionally, we'll explore how RapidFort's SASM approach can further reduce runtime and development costs.



## 1

Understand the security risks associated with CI/CD pipelines.

## 2

Explore the benefits of leveraging scanning tools and curated container images to mitigate risks.

## 3

Discover RapidFort as a one-stop shop for CI/CD security needs.

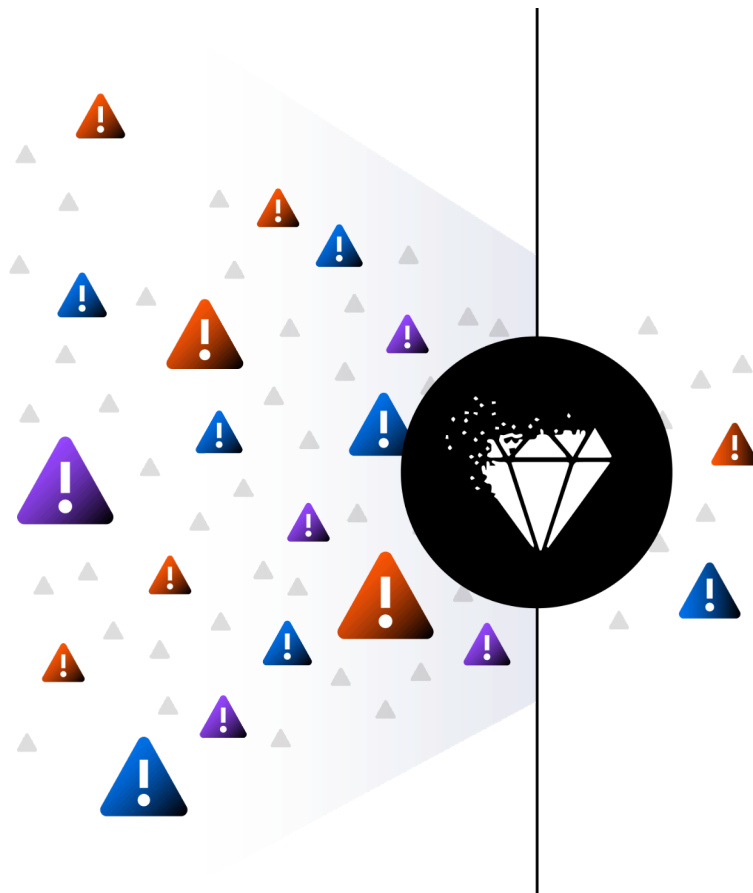
## 4

Learn best practices for integrating security into the CI/CD process.

## The CI/CD Security Challenge

The agility and efficiency of CI/CD pipelines have revolutionized software development. However, this rapid release cycle can introduce security vulnerabilities if not properly addressed. Here are some key challenges:

- **Speed vs. Security:** The pressure to release new features quickly can lead to security testing being rushed or skipped altogether.
- **Integration Complexity:** CI/CD pipelines often involve a complex ecosystem of tools. Vulnerabilities within these tools themselves can become an entry point for attackers.
- **Shifting Security Left:** Traditional security practices focused on post-development testing. Integrating security checks throughout the CI/CD pipeline requires a cultural shift and additional training for developers.
- **Version Control and Dependency Management:** Rapid development can lead to frequent code changes and updates to dependencies. Managing versions and ensuring compatibility becomes crucial to avoid introducing vulnerabilities or conflicts.
- **Lack of Visibility:** Complex pipelines can create a lack of visibility into the software lifecycle. This makes it difficult to track potential security risks or identify the source of issues during deployment.



## RapidFort: Your Complete Vulnerability Management Solution

RapidFort offers a comprehensive solution that addresses all aspects of CI/CD vulnerabilities, eliminating the need to manage multiple vendors and tools. Here's how RapidFort streamlines your security efforts:

- **Curated Container Images:** RapidFort provides access to a library of hardened and curated open source images. These images with near zero CVEs, containing only the necessary components and minimized attack surfaces. Additionally, RapidFort ensures these images are kept up-to-date and are:

- Hardened NIST 800-70
- FIPS 140-2 / 140-3 validated
- RF Justification for Plan of Action and Milestones (POAMs)
- Fresh images daily

- **Instrument and profile - Integrated SCA Scan and DevTime Protection tools:**

RapidFort's platform seamlessly integrates with your CI/CD pipeline.

These tools can scan code for common vulnerabilities, identify open-source component risks, and analyze container images for suspicious content. All within a single, unified platform.

Highlights:

- Generate SBOM and RBOM
- Prioritize vulnerability remediation
- Integrated CIS / STIG Benchmarks
- Filter noise with RapidFort advisory

- **Hardening and Defending - Automatic Scanning and RunTime Protection tools:**

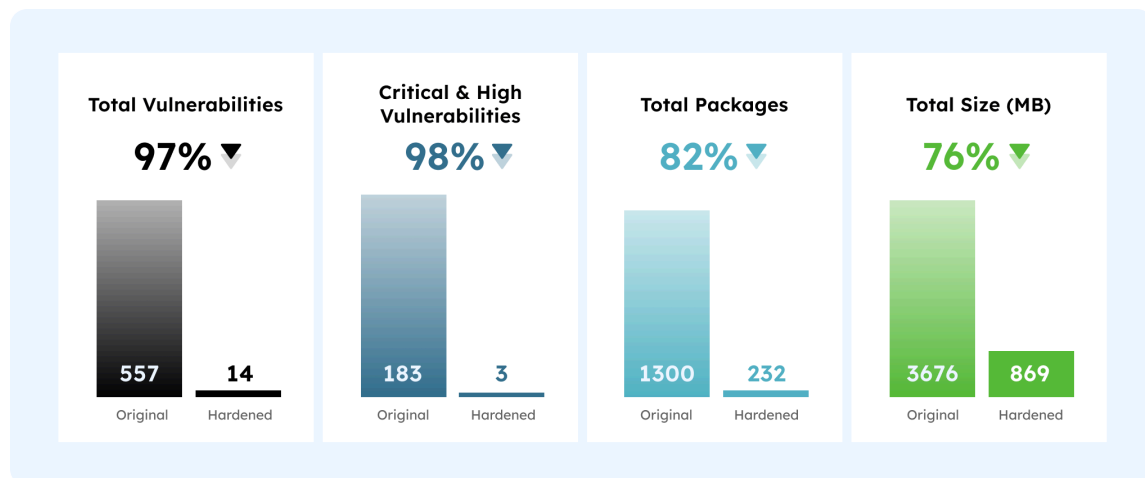
A key advantage of RapidFort is its ability to automatically scan container images during the build process (build time) and while the application runs (runtime). This identifies unused code that can harbor vulnerabilities. RapidFort then automatically hardens the containers by removing this unnecessary code, potentially remediating up to 95% of software vulnerabilities. This significantly reduces your attack surface and streamlines the development process by eliminating the need for developers to manually identify and remove unused code.



## Benefits of a Unified CI/CD Vulnerability Management Solution with RapidFort

By adopting RapidFort as your complete CI/CD security solution, you can achieve several benefits:

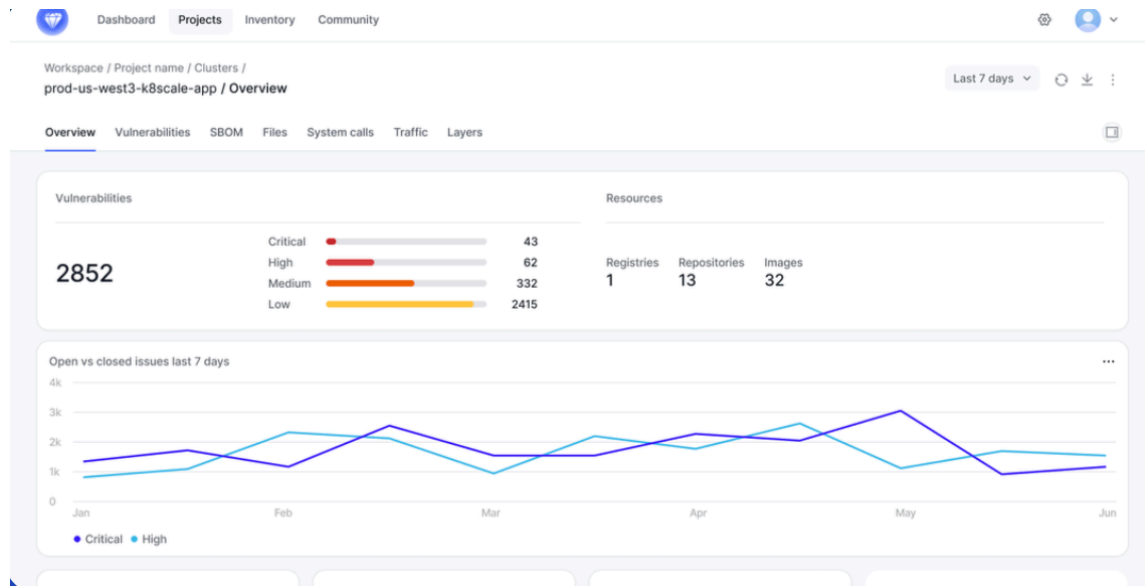
- **Reduced Complexity:** Eliminate the need to manage multiple vendors and tools for scanning, curated container images, and SASM. RapidFort provides a single platform for all your CI/CD vulnerability management needs.
- **Improved Efficiency:** Streamlined workflows, automated scanning and hardening processes within RapidFort's platform save development teams valuable time and resources.
- **Enhanced Security Posture:** The combination of curated container images, integrated scanning tools, and SASM capabilities from RapidFort significantly strengthens your overall security posture by reducing the attack surface, identifying vulnerabilities early, and automatically hardening containers to minimize potential exploits.
- **Faster Time to Market:** By leveraging hardened and curated container images, and automating vulnerability remediation, RapidFort helps you deliver features to market faster with reduced security risks.
- **Improved Compliance:** RapidFort's SASM platform can generate Software Bill of Materials (SBOMs) and RBOMs™. SBOMs provide a complete list of all software components used in your application, while RBOMs take it a step further by identifying the actual code that is executed at runtime. This comprehensive visibility helps with vulnerability management and ensures compliance with industry regulations.



## Cost Savings with RapidFort SASM

Beyond the security benefits, RapidFort's SASM approach offers significant cost savings in two key areas:

- **Reduced Runtime Costs:** By eliminating unused code through container hardening, RapidFort optimizes the size and resource consumption of your containerized applications. This translates to lower runtime costs in cloud environments where billing is often based on resource usage.
- **Improved Development Efficiency:** Automated scanning and hardening processes within RapidFort's platform free up valuable developer time. Developers can focus on core functionalities and innovation rather than manual security audits or code optimization tasks.

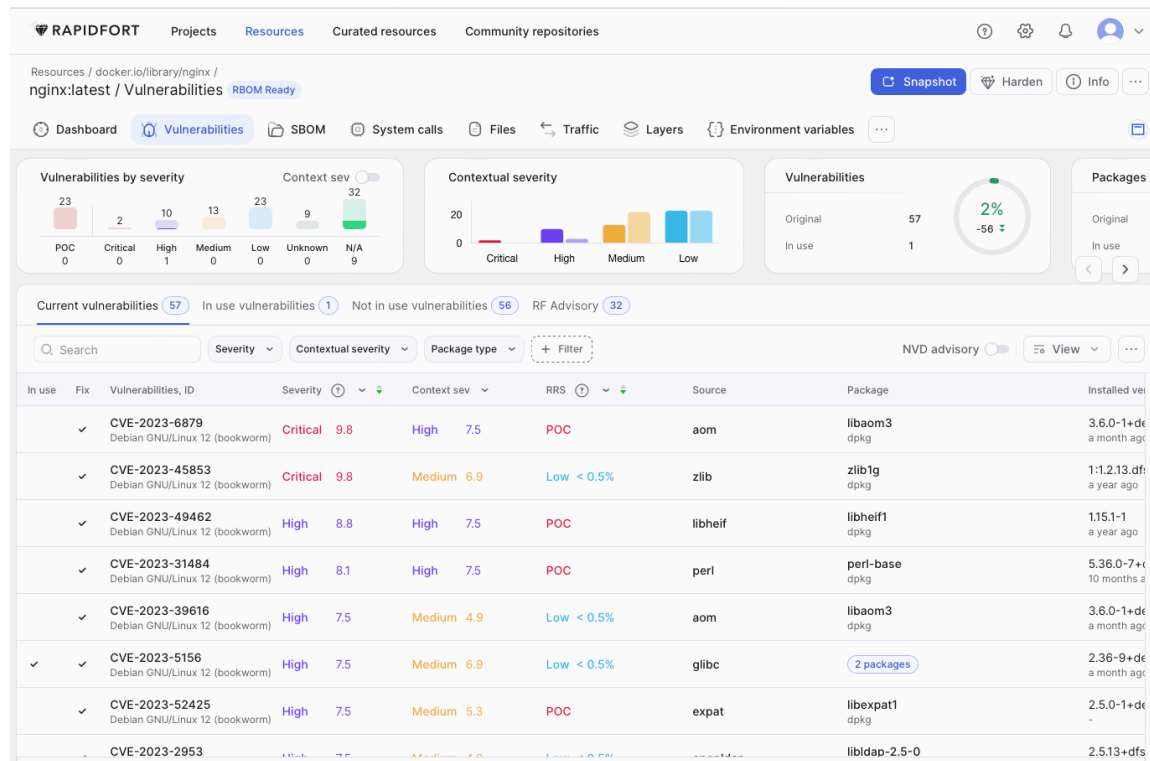


## Conclusion

RapidFort empowers organizations to achieve a balance between rapid development and robust security within CI/CD pipelines. This white paper has explored the challenges of CI/CD security and introduced RapidFort as a comprehensive solution. By implementing RapidFort, you can streamline your CI/CD security processes, strengthen your software development lifecycle, deliver secure features with confidence, and potentially reduce development and runtime costs.

## Take Control of Your CI/CD Security Today

Visit RapidFort's website at [www.rapidfort.com](https://www.rapidfort.com) or contact us to learn more about how we can help you secure your CI/CD pipeline and deliver innovative features with confidence.



Copyright © 2024 RapidFort Inc.

[www.rapidfort.com](https://www.rapidfort.com)

