RAPIDFORT

The Future of Container Security

How RapidFort Scanner Outperforms Industry Leaders

Table of Contents

Executive Summary

In recent years, Software Attack Surface Management (SASM) has become a critical focus for organizations striving to maintain robust security postures. As the foundational step in developing a successful software security program, vulnerability scanning provides essential clarity by identifying potential weaknesses within software systems, allowing proactive remediation to mitigate risk. This is why accurate scanning is crucial, showcasing true risks that need remediation and thus fortifying an organization's defensive posture.

While various techniques exist for scanning software, such as internal and external scanning or compliance scanning, RapidFort stands out by employing a combination of patented mechanisms to achieve unparalleled reliability and accuracy. This cutting-edge approach not only provides the most dependable results but also empowers customers to consolidate multiple scanners into one, significantly reducing compute requirements and eliminating false positives.

This case study presents a comparative analysis of RapidFort against three industry-leading scanners, as per DoD customer requirements. The study involved a rigorous 20-container test designed to evaluate the performance and accuracy of each scanner. Key findings from the study reveal that RapidFort outperforms all three competitors, demonstrating superior accuracy and reliability in vulnerability detection.

As we delve deeper into the study's methodology and comparative analysis, it becomes evident that RapidFort's innovative approach to vulnerability scanning sets a new standard. Embrace the power of precision, consolidate your scanning needs, and take a proactive stance against potential threats – the future of security starts with RapidFort.

Study Highlights:

- **RapidFort delivered the most accurate results in the study, successfully detecting all known vulnerabilities without introducing false positives or false negatives.**
- **The other three scanners exhibited varying levels of detection accuracy, with some missing critical vulnerabilities and others generating false positives that could lead to unnecessary remediation efforts.**
- **These findings underscore the importance of precision in vulnerability scanning—minimizing both false positives and false negatives is essential to maintaining an effective and efficient security posture.**

Introduction

Software and applications are the lifeblood of modern organizations, but in recent years, the industry has shifted away from traditional virtual machines to embrace containerization. The Application Container Market and Containers as a Service (CaaS) Market are both projected to grow at compound annual growth rates of over 30% in the next five years, reflecting the widespread adoption of container technology across both public and private sectors.

This rapid adoption underscores the urgent need for robust security measures tailored to containerized environments. Research indicates that 50% to 90% of software within production environments remains unused. These dormant components frequently include known vulnerabilities—providing bad actors with opportunities to exploit systems, exfiltrate data, or gain persistent access while remaining undetected.

In this context, vulnerability scanning plays a critical role. Scanners must not only detect a wide range of vulnerabilities, but also deliver precision—identifying real threats while minimizing noise from false positives and missed detections. As organizations strive to meet compliance standards, adopt DevSecOps practices, and manage growing software supply chains, the effectiveness of these scanners becomes central to maintaining security posture.

This study was designed to evaluate the performance of RapidFort's vulnerability scanner against three industry leaders as per DOD requirements. With a methodology aligned to real-world use cases—including container images drawn from popular open-source registries and a range of operating systems—the goal was to measure detection fidelity across consistent baselines.

By providing clarity on scanner performance in terms of both breadth (number of tests passed) and depth (accuracy within those tests), this report enables security professionals to make informed, data-driven decisions about their vulnerability management strategies.

Methodology

To effectively evaluate RapidFort's vulnerability scanner performance against three industry-leading competitors, extensive testing was conducted across 20 container images encompassing a diverse range of programming languages and operating systems. This structured approach was designed to ensure a balanced, real-world, and comprehensive assessment of each scanner's detection capabilities across varied technical environments.

Study Design

In our methodology, the diversity and range of programming languages and operating systems used mirrored real-world containerized applications. By incorporating this variety, we ensured the study provided a holistic evaluation of each scanner's performance across different technical landscapes.

The selection of container images was meticulously curated to represent commonly used and high-value containers in both government and commercial sectors. This included popular open-source images favored by developers, ensuring that the tests were both relevant and reflective of typical usage scenarios.

Scoring System

To objectively compare scanner performance, we implemented a robust scoring system. Each test (container image) contained a set of predefined vulnerabilities, which served as the Ground Truth (GT). The scanners were tasked with identifying these vulnerabilities, and their results were then compared against the GT. Points were awarded based on correct matches to the GT. Specifically:

- A scanner received one point for each correctly identified vulnerability.
- No points were awarded for incorrect or missed vulnerabilities.

Given that each test varied in the number of embedded vulnerabilities, it was essential to normalize the scoring to ensure fairness. We achieved this by calculating both the number of tests correctly scored and the total number of vulnerabilities accurately identified. This dual-metric approach provided a comprehensive view of each scanner's performance, accounting for both breadth (number of tests) and depth (number of vulnerabilities).

Summary of Results

RAPIDFORT

100%

Overall accuracy rates

Scanner A
74%

Scanner B
86%

Scanner C
51%

The results of our comparative study reveal significant differences in the performance of the three vulnerability scanners. RapidFort consistently outperformed all three competitors, demonstrating superior accuracy and reliability in vulnerability detection.

Performance Metrics

Our evaluation showed that RapidFort scored better than Scanner A in all 20 tests, outperformed Scanner B in 19 tests, and surpassed Scanner C in all 20 tests. The overall accuracy rates were as follows:

- **RapidFort:** 100%
- **Scanner A:** 74%
- **Scanner B:** 86%
- **Scanner C:** 51%

Implications of Findings

The high accuracy rate achieved by RapidFort has significant implications for vulnerability detection and overall security posture. In the context of vulnerability scanning, accuracy is paramount—it ensures that true risks are identified and addressed while minimizing the operational noise caused by false positives and reducing exposure from undetected vulnerabilities due to false negatives.

Reduction of False Positives:

High accuracy in vulnerability detection reduces the number of false positives—incorrect identifications of vulnerabilities that do not actually exist. These inaccuracies can overwhelm security teams, wasting valuable time and diverting attention from genuine threats. In fact, 44% of organizations report spending over 21 hours per week remediating CVEs.

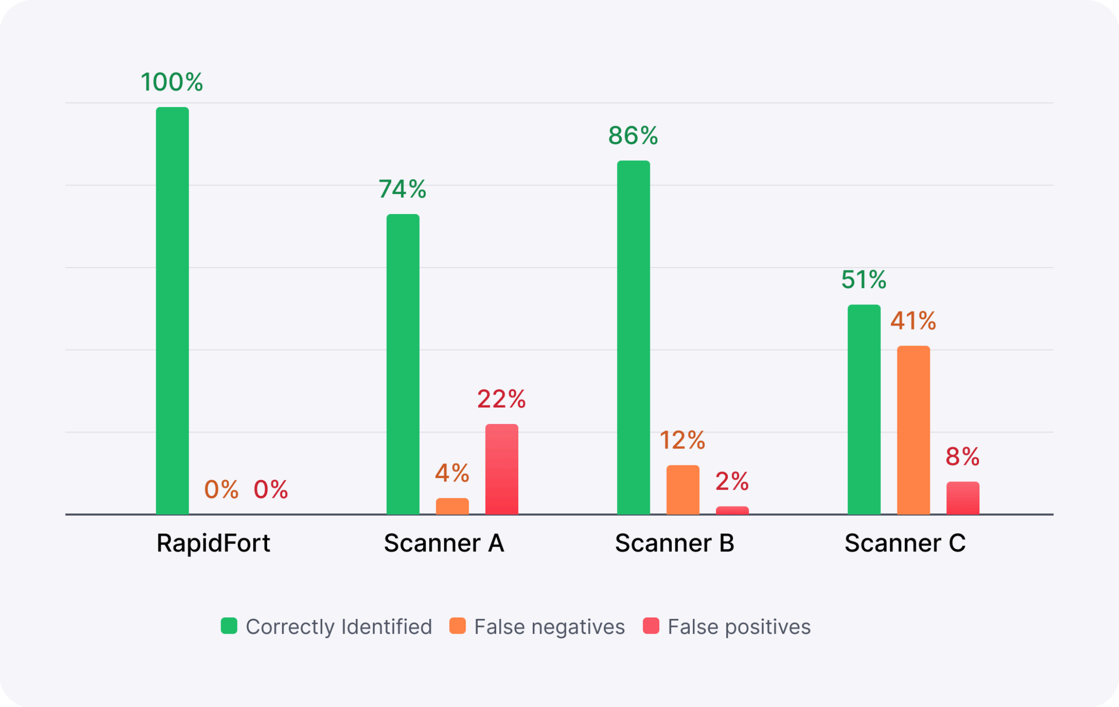
By minimizing false positives, RapidFort enables security teams to focus on real, actionable issues, improving both the efficiency and effectiveness of vulnerability management workflows.

Reduction of False Negatives:

Equally important is minimizing false negatives, which occur when actual vulnerabilities go undetected. These pose a serious risk, as they leave critical issues unaddressed—potentially exposing organizations to exploitation.

RapidFort's superior detection accuracy significantly reduces false negatives, ensuring that fewer vulnerabilities are overlooked. This enhances the overall security posture of containerized applications and helps safeguard production environments from undetected threats.

In summary, the results of our study clearly demonstrate that RapidFort sets a new standard for vulnerability scanning within containerized environments. Its superior accuracy and reliability make it an invaluable tool for organizations seeking to strengthen their security posture and protect containerized workloads against evolving threats.



Why You Should Run with RapidFort

The findings from our study not only underscore RapidFort's superior performance but also highlight the distinct strengths that enable it to excel in vulnerability detection. These strengths—rooted in advanced technology and comprehensive methodologies—translate into tangible, real-world benefits for securing containerized environments.

Comprehensive Package Detection:

RapidFort employs proprietary techniques to achieve deep and comprehensive package detection. This includes identifying all files and packages—whether or not they are managed by a package manager—as well as binaries, associated vulnerabilities, and their dependencies within a containerized application.

By thoroughly scanning and analyzing these components, RapidFort ensures that no potential vulnerabilities are overlooked during security analysis.

Superior Vulnerability Database Quality:

RapidFort curates and integrates data from a wide range of trusted sources, intelligently filtering out noise caused by false positives and exposing false negatives. This meticulous curation enables the scanner to accurately match identified packages with known vulnerabilities, delivering dependable results that security teams can trust.

Additionally, RapidFort's advisory system provides clear justification when a vulnerability is deemed not applicable, along with direct references to the original sources from which those justifications were derived.

Real-World Impact

The importance of these strengths becomes evident when considering the real-world consequences of inaccuracies in vulnerability detection. Missing critical vulnerabilities due to false negatives can result in severe outcomes, as illustrated by the recent high-profile incident involving a backdoor in XZ Utils, a widely used utility. When a scanner fails to detect such a vulnerability, it leaves the organization exposed to exploitation and significantly increases the risk of security breaches.

Conversely, an overabundance of false positives can overwhelm security teams, forcing them to waste valuable time and resources chasing non-existent threats. This not only reduces operational efficiency but also increases the likelihood that genuine vulnerabilities will be overlooked. RapidFort’s high detection accuracy helps mitigate both risks, allowing security teams to focus on addressing real issues and maintaining a resilient security posture.

About Us

At RapidFort, we are dedicated to empowering organizations to enhance their container security and vulnerability management practices. As a leading provider of cloud-native cybersecurity solutions, we combine Near-Zero CVE Images with our CI/CD-native SASM platform to remove up to 95% of CVEs automatically, with no code changes—helping teams reduce their attack surface and secure containerized environments.

We trust that the insights presented in this report will aid organizations in gaining a deeper understanding of their security landscape and taking proactive steps to fortify their defenses.

To learn more about the RapidFort platform, please visit www.rapidfort.com