RAPIDFORT

The State of Container Security

OSS Vulnerability Management, Containerization, and Shift Left: Insights from RapidFort's Comprehensive Survey

Containerization is on the rise in the software industry, but this shift has come with increased security risks. RapidFort surveyed organizations to understand their container security practices and secure application delivery. In this document, we have analyzed the results, and have provided our own recommendations for containerization.

Foreword

Today's software environments present significant risks to organizations, with 50% to 90% of software going unused, yet still continuously maintained and open to security threats. Most of this risk comes from vulnerabilities present in open source software, which represent the bulk of modern applications and must be managed differently from in-house or vendor software

Unfortunately, the scanning solutions in today's market offer limited effective prioritization methods beyond identifying vulnerabilities by category, leaving security teams overwhelmed and needing practical tools to manage the risk associated with software vulnerabilities.

At RapidFort, we have developed the industry's first Software Attack Surface Management platform to help organizations understand and harden their software infrastructure. Our SASM platform allows security teams to observe and manage software components, making informed decisions about their risk management strategies. By choosing RapidFort, organizations can proactively manage their software infrastructure and reduce the risk of data breaches and other cyber attacks.

We hope you consider these insights and findings as you build your vulnerability management strategies.

— Mehran Farimani, CEO

Introduction

In recent years, the software industry has been shifting away from traditional virtual machines and embracing containerization. Containerized applications offer significant advantages, such as efficient resource utilization, flexibility, and scalability. Containers are a lightweight, efficient option for software development and deployment, and often contain a substantial amount of free, open source software (OSS).

The rise in OSS usage and containerized workloads has yielded a complex software attack surface, presenting a seemingly insurmountable challenge for security teams to manage risk. There are many OSS vulnerabilities that security teams must assess, prioritize, and address continuously with limited resources. In addition, DevOps adoption is exacerbating this problem as the software is rapidly changing.

As a result, security teams face the difficult task of reducing significant risks for their organizations, while needing clarity and the proper tooling to do so effectively. It has become critical for many organizations to prioritize container security and implement modern vulnerability management practices with efficacy.

Different ideas exist on how to approach container security, including when to implement security measures during software development and who should oversee them.

As a modern cybersecurity company, RapidFort sought to gain insights into the current state of container security and vulnerability management practices. We surveyed industry professionals to learn about how organizations handle the shift towards containerization and what steps they take to ensure their applications are delivered and deployed securely and efficiently.

Methodology:

The survey targeted 100 IT professionals and security practitioners (55 male, 45 female) across various industries. 91% of those surveyed were between the ages of 25 and 44. PollFish, an online survey platform, was used to conduct the survey, which consisted of multiple-choice and open-ended questions. The survey was designed to gather information on the respondents' familiarity with containers, their vulnerability management practices, and other related inquiries.

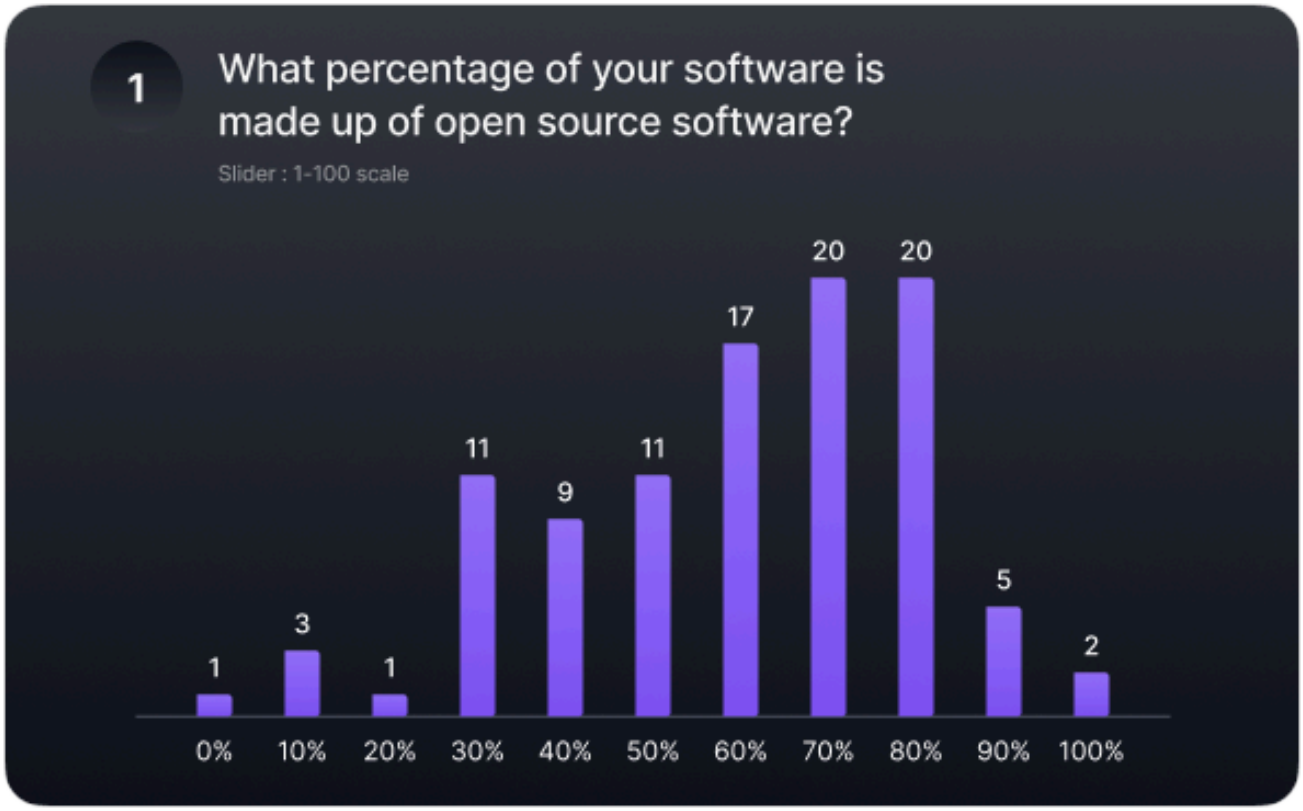
Key Findings:

Companies operate within a mixed environment:
While the mean percentage of containerized workloads in the respondents' organizations is nearly 40%, more than a third of applications run on VMs, and over 30% classify as serverless.

Broad adoption of open source software:
75% of respondents reported that at least half of their software is open source. As most containers have open source software, this can be a factor in the high open source utilization, and a potential flashpoint for security concerns.

Security and dev teams share vulnerability ownership:
43% of respondents said developers and security personnel own vulnerability management in their companies.

CVE Management takes up a significant amount of company time:
73% of people said that their organizations spend between 11 and 30 hours each week remediating each prioritized CVE.



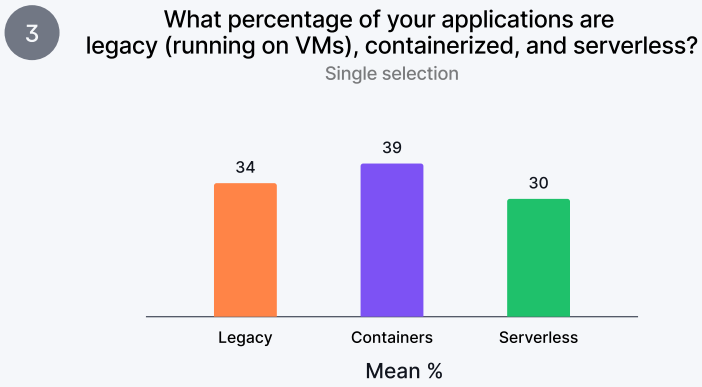
Challenges and Expectations

The responses garnered from the survey are an informative look into the state of container security while providing valuable insights into related issues, such as CVE remediation, the "Shift Left" approach, and the delegation of vulnerability management.

Container Security: Three main issues

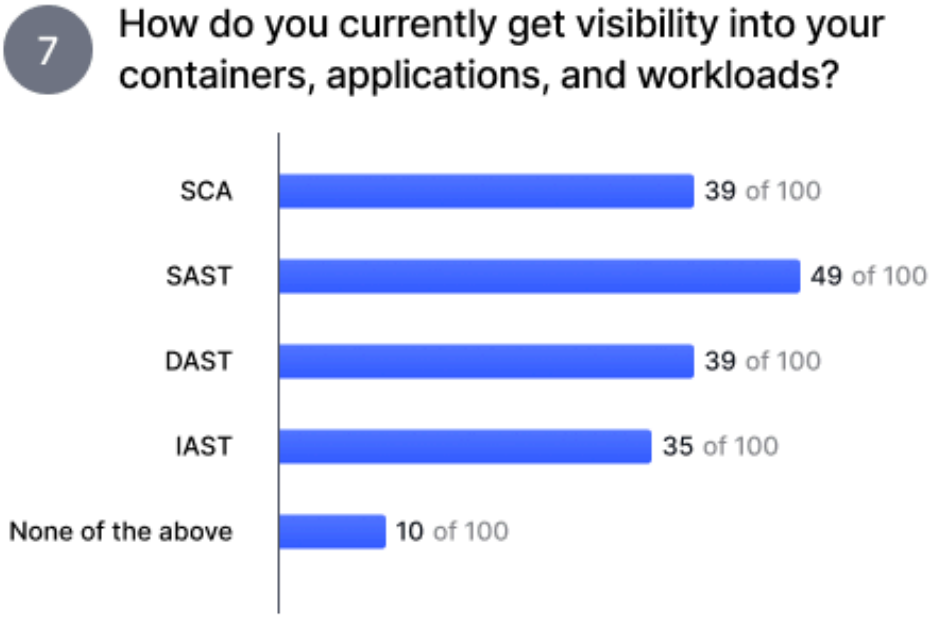
Respondents frequently mentioned three challenges that they face in securing containers, applications, and workloads:

Implementation:
With many organizations still running a large portion of their applications running on VMs, it is reasonable to expect container adoption to be challenging, as VM-to-container migration is rewarding but complex. Proper developer and security tooling are integral to aiding this migration.



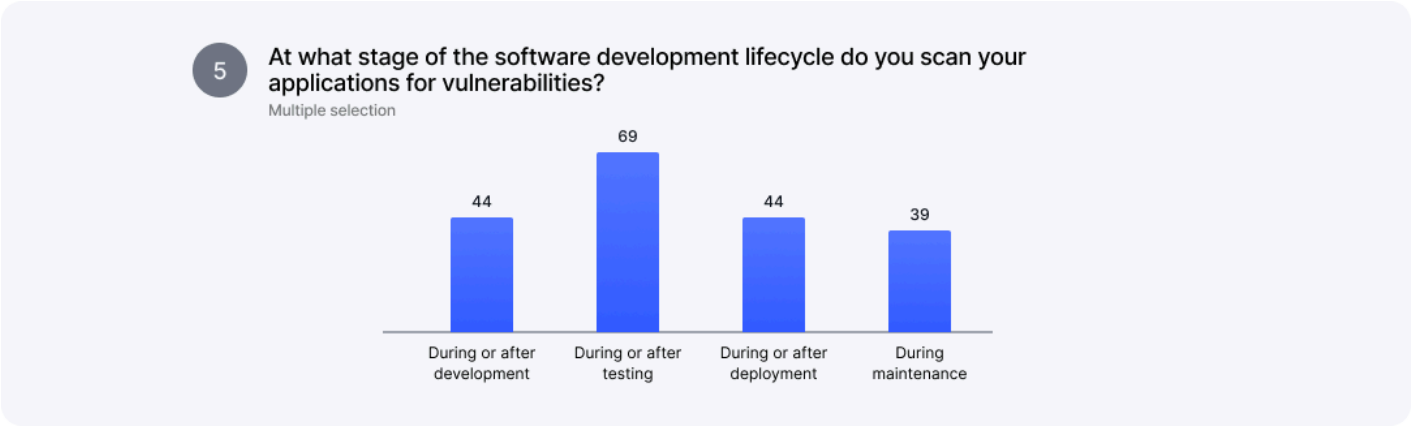
Vulnerability Remediation:

Vulnerability monitoring and remediation present unique challenges to organizations. Respondents use several methods to gain visibility into software vulnerabilities, including SCA (Software Composition Analysis), SAST (Static Application Security Testing), DAST (Dynamic Application Security Testing), and IAST (Interactive Application Security Testing). SAST – which allows for automation, efficient results, and early detection – proved to be the most popular answer, with 49% of respondents reporting this as the method their companies utilize to gain an understanding of their security posture.



Automation:

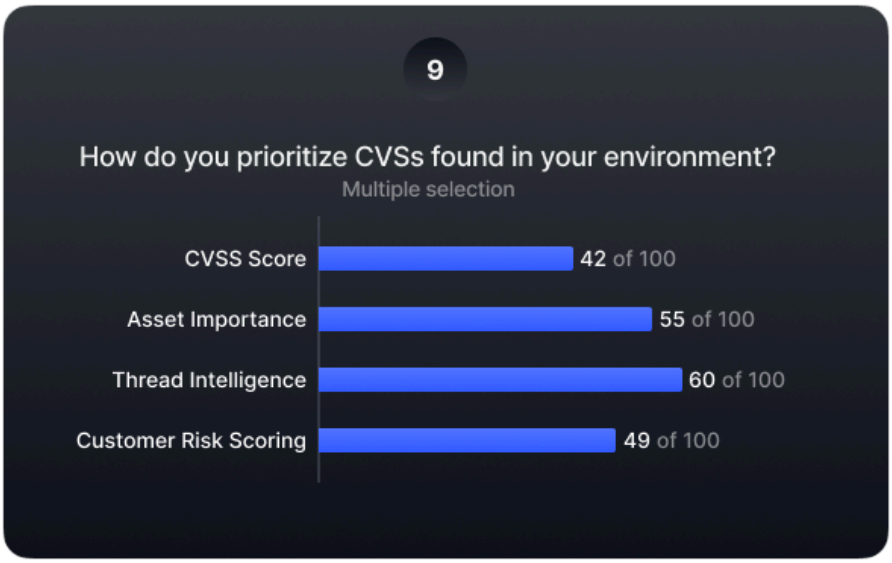
Automation encompasses the scheduling, resource allocation, and scanning of containers, and it was identified as the most prominent issue among the respondents. While cited as a critical issue, automation is the primary solution to problems related to human-based container monitoring. As the number of containers an organization uses increases, the need for automation becomes ever more significant to ensure each container functions well without the additional resource drain of human oversight.



Security Practices and CVE Remediation

In understanding what security issues and vulnerabilities respondents deal with, it is essential to know how they deal with these issues, including how they are prioritized, at what stage in SDLC, who is responsible for vulnerabilities, and how much time is spent on these issues.

CVE Prioritization

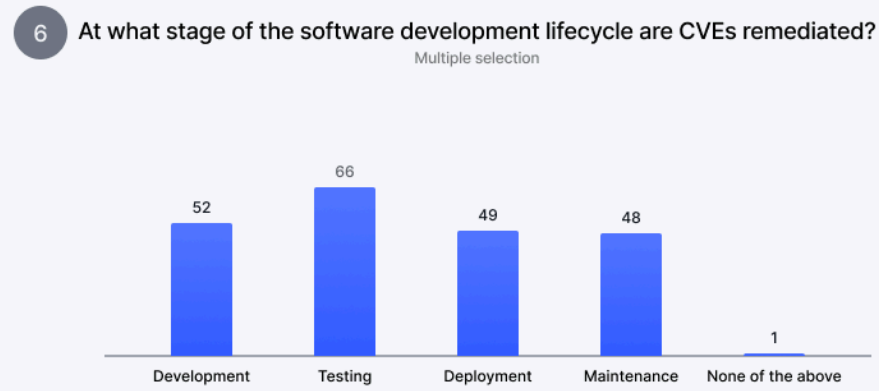


With so many potential pain points in container security and CVE remediation incurring a significant resource drain for security teams, prioritization of vulnerabilities is crucial for any organization that utilizes containers. The respondents listed several ways their organizations prioritize CVEs, including the value of the impacted asset, the CVSS (Common Vulnerability Scoring System, an industry standard for assessing vulnerabilities), and custom risk scoring exclusive to each respondent's respective company. Tellingly, the most widely mentioned method (utilized by 60% of respondents) was threat intelligence, indicating that companies prioritize CVE remediation around the potential harm that can arise from these vulnerabilities being exploited.

When Vulnerabilities are Scanned and Remediated: Shift Left Adoption

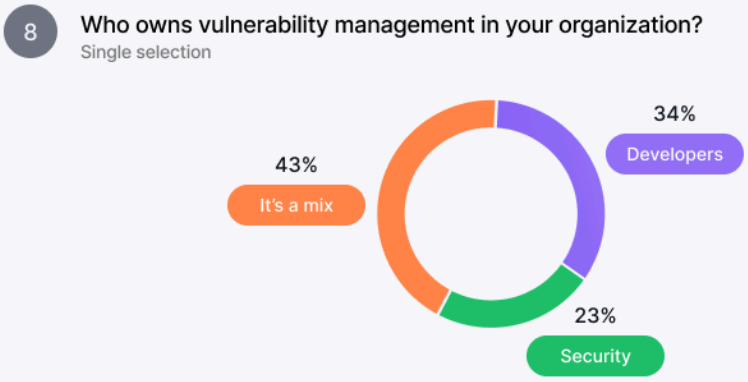
Scanning during testing is in line with best practices for application security. It is reassuring that 69% of respondents reported that their companies scan their applications for vulnerabilities during or after a defined "testing phase" of the software development lifecycle. In addition, 66% of respondents reported that testing is also conducted when CVEs are remediated.

What is more interesting may be that companies also opted to scan and remediate vulnerabilities during development or deployment at equal rates. Scanning and remediation associated with the earlier stages of the software development lifecycle are consistent with the "Shift Left" approach, which seeks to deal with software issues as early as possible. Shift Left aims for testing done early and often to identify and curb potential vulnerabilities before remediation becomes more expensive at later stages.



While RapidFort is a proponent of the Shift Left approach, we understand the issuesassociated with its effectiveness and the considerable effort and resources needed for successfulimplementation. RapidFort is committed to helping companies Shift Left without adding more work or resource drain to development teams, but we also understand why many companies are not yet able to fully commit to Shift Left.

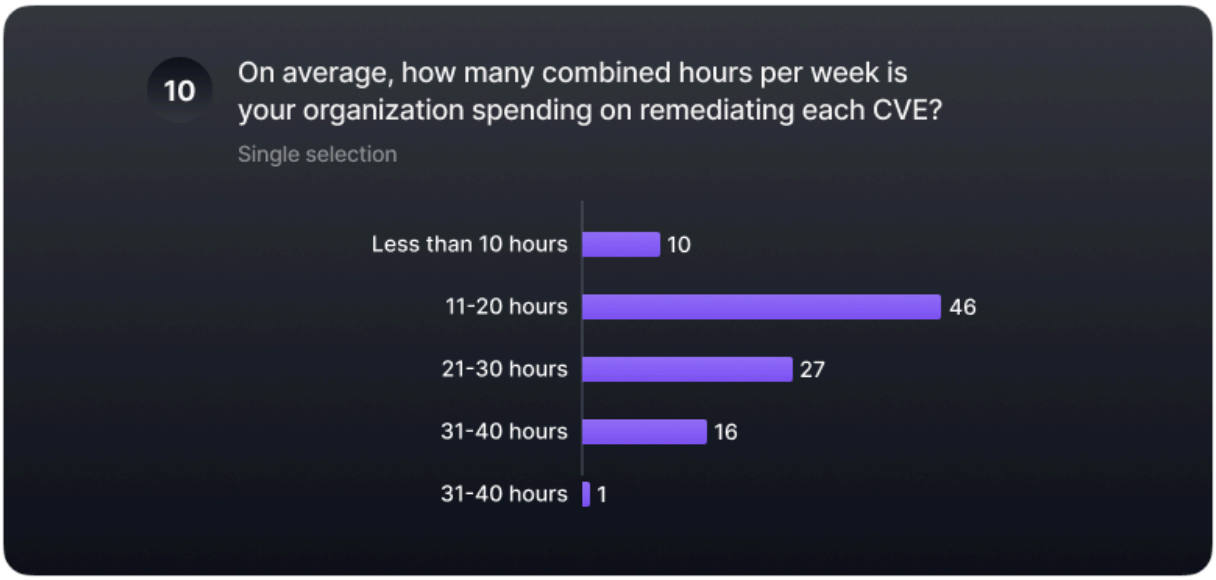
The owning of vulnerability management



The survey suggests that many companies view vulnerability management as a shared responsibility, with nearly half (43%)of the respondents stating that a mix of security professionals and developers own vulnerability management at their companies. RapidFort is a strong believer in a hybrid approach to vulnerability management, so it is gratifying to see this approach of shared accountability being adopted by respondents' organizations.

Hours Spent on CVE Remediation: A Time Drain

An illuminating result from this survey was how much time companies spend remediating CVEs, which highlights the drain these vulnerabilities can have on an organization's time and resources, and how important time-saving security tools can be to alleviate these issues.



44% of respondents reported their companies spend over 21 hours a week on remediating each CVE, while only 10% reported that their employers spend 10 hours a week or less on these issues. For companies with a frequent release cadence and limited bandwidth, spending 3 or more hours a day on individual CVE remediation is a costly use of time. Ensuring the proper security resources are employed (such as RapidFort's SASM platform, which can identify and remove roughly 80% of vulnerabilities in the execution path) to mitigate this time spent should be an essential priority for any applicable organization.

Strategies for Improving Container Security

To address the challenges spanning container security and CVE remediation, RapidFort recommends implementing a "Shift Left" approach to vulnerability management where security is integrated early in the software development life cycle. This approach enables organizations to identify and remediate vulnerabilities early, reducing the risk of attacks, minimizing the impact on production environments, and saving substantial resources in the aggregate. Our SASM platform provides an instant reduction in attack surface by 60-90%, and makes the transition to a Shift Left approach as seamless and cost effective as possible.

Additionally, RapidFort recommends an increased focus on automation. While cited as the biggest hardship when it comes to container security, using CI/CD pipelines to automatically scan and remediate those vulnerabilities in the SDLC can significantly reduce the time spent on vulnerability management, allowing teams to focus on other critical tasks.

Moreover, RapidFort recommends implementing a hybrid ownership model for vulnerability management, where both security and development teams are involved. This ensures that vulnerabilities are identified and remediated promptly – reducing the risk of complications – while also creating a culture of shared accountability and responsibility throughout an organization.

Conclusion

The survey results provide an enlightening look into the challenges associated with container security and vulnerability management. As containerization continues to grow in popularity, the need for effective security practices becomes even more critical. Faced with a plethora of potential security issues and vulnerabilities, security teams are tasked with discerning what is most important, and how best to proceed.

Organizations must address the challenges outlined in the survey – including the need to manage third-party CVEs, prioritize remediation efforts, and ensure visibility into containers and workloads – to ensure their systems and data remain secure.

At RapidFort, we provide organizations with the solutions to remediate these problems. With proprietary tools such as our SASM platform, we can empower your organization to commit to container automation, a hybrid ownership of vulnerability management, and a Shift Left approach to software testing, without severely draining security bandwidth or pulling your teams away from more important work. By adopting these best practices, organizations can tackle container security without overwhelming their security teams or depleting their resources.

About us

At RapidFort, we are committed to helping organizations address their container security and vulnerability management needs. As a cloud-native cybersecurity company specializing in container security, we understand the unique challenges of securing modern software environments and offer innovative solutions to help our clients protect their software infrastructure. We hope that the insights provided by this survey will help organizations better understand the challenges they face and take steps to address them.

Visit our website to learn more.