Checkmarx

EBOOK

6 Key Considerations for Container Security

Choosing the Right Container Security for Your AppSec Program

6 Key Considerations for Container Security

At a glance

- Can the solution inspect container image layers?
- Is the solution able to correlate data from all stages of the SDLC?
- Does it perform triage and automatic prioritization?
- Is the solution part of a consolidated platform?
- Can it provide tangible remediation suggestions?
- Does the solution allow for integration? And is it developer centric?

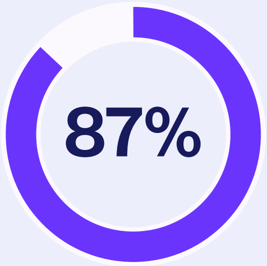
Contents

Securing Containers

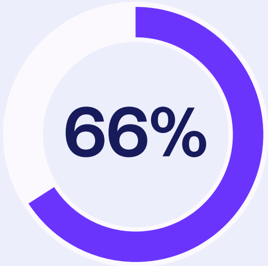
Overview

Containerization has become a dominant force in application development, delivering agility, scalability, and efficiency gains. However, it presents unique security hurdles. Unlike traditional applications, containers create a dynamic and distributed interconnected environment, which significantly increases the attack surface and exposes systems to new risks.

Securing containers is more critical than ever. While pulling images from public repositories is convenient, it also introduces potential vulnerabilities, such as malware injection. Inadvertent exposure of sensitive data within container registries can lead to severe data breaches.



of container images
have high or critical vulnerabilities.



of organizations
have faced security issues from insecure container images.

Sysdig 2023 Cloud-Native Security and Usage Report

Effective security practices are a must, especially since Gartner predicts that more than 95% of organizations will adopt containerized applications by 2028. Addressing these challenges requires comprehensive security measures across all layers of the container ecosystem—from code to image management to runtime environments.

So where do you start? Here are the top things you should keep in mind when it comes to container security. By understanding and implementing these practices, you can effectively mitigate security risks and harness the full potential of containers. We'll focus on critical areas like securing container images by breaking them down into layers, triage and prioritization, and remediation, combining insights from across the Software Development Lifecycle (SDLC) and the importance of a consolidated platform and developer experience.

Keep reading about **Checkmarx container security**

01

Identifying Risk at Every Layer of the Container

Container images are comprised of multiple layers, and each layer can potentially introduce security concerns. The base image serves as the foundation, and any vulnerabilities here can propagate throughout the container. Software dependencies add complexity, and often, harbor additional risks. Finally, the application code itself may contain bugs or security flaws. By separating the image into these layers, we can pinpoint the exact location of these threats.

When choosing a container security solution, prioritize one that analyses each image layer for vulnerabilities. This in-depth analyzes examines the base image, its software dependencies, and the application code itself. By breaking down the container into these distinct components, you will gain a better understanding of the security risks within each component. This targeted approach allows for more effective remediation strategies.

RECOMMENDATION

Consider a solution that can analyze each container image layer for targeted vulnerability remediation

02

The Power of Triage and Prioritization

Triage and prioritization are the key for managing vulnerabilities in containerized environments. Triage involves categorizing vulnerabilities by severity, exploitability and potential impact on the application. Prioritization ensures critical vulnerabilities are addressed first, reducing the overall risk. This systematic approach allows security teams to allocate resources efficiently, focusing on the most pressing security issues that threaten the integrity of containers and their applications.

You can probably easily picture a security team overwhelmed by a constant stream of vulnerability alerts. Can you filter out the noise by highlighting the most critical threats? The solution you choose needs to be able to prioritize vulnerabilities based on risk, assess the likelihood of exploitation (such as by correlating pre-production and runtime insights), and consider the potential business impact by correlating all stages of the SDLC with runtime information.

This allows teams to optimize resource allocation, focusing on the most important issues first. Choosing a solution with triage and prioritization capabilities results in reduced response times, and your overall security posture is strengthened by proactively addressing the vulnerabilities that matter most.

RECOMMENDATION

Choose a solution that can prioritize vulnerabilities by correlating pre-production and runtime insights

03

Remediating the Entire Container Lifecycle

It is not enough to settle for a container security solution that just identifies vulnerabilities. Focus on one that offers actionable remediation insights, that will allow you faster patching, reduce the attack surface, and allow the integration of all security aspects together.

Faster Patching:
Identifying a vulnerability is only half the battle, you also must remediate it in your source code or open source library. So, it is critical to have a solution that can pinpoint the vulnerable code within your container through a direct integration with the code repositories and running containers. Having actionable insights, like specific patches or less vulnerable image recommendations, empowers developers to prioritize and fix issues quickly.

Reduced Attack Surface:
Every unpatched vulnerability is a potential security breach waiting to happen. Recommending a less vulnerable image streamlines remediation, which minimizes the window where attackers can exploit the flaw.

Developer-First Security:
Weaving vulnerability remediation into the development lifecycle fosters a "security-first" culture. Developers using the Docker Desktop Extension can address issues early, preventing them from becoming larger problems once in production environments.

A proactive approach to vulnerability remediation strengthens your container security posture. Choose a solution that empowers you to fix problems quickly, minimizing risks and ensuring smooth application operation.

RECOMMENDATION

Prioritize a solution with actionable remediation insights within the development cycle for faster vulnerability fixes

04

Ability to Correlate Insights From All Stages of the SDLC

Organizations looking for a container security solution should prioritize its ability to integrate security measures across the Software SDLC. This entails embedding security from initial design and development through testing and deployment phases, including IDEs, SCM tools, CI/CD tools, and feedback tools.

Integrating with runtime is important for prioritizing vulnerabilities and helping developers focus on what matters the most by reducing alert noise. Such integration allows for automatic security scans as applications progress from code to build to deploy in the cloud and increases security coverage throughout the application lifecycle, minimizing the likelihood of introducing vulnerabilities during development cycles. The chosen solution must be able to correlate all security data, for instance detecting internet exposure and vulnerable OSS packages in running containers. The solution needs to be able to identify risk across your entire footprint – including cloud-native and traditional non-cloud applications.

By prioritizing SDLC integration and scalability, you can strengthen your organization's security posture and build better containerized applications.

RECOMMENDATION

Prioritize a solution with the ability to integrate in all stages of the SDLC

05

Container Security as Part of a Platform

Why? Because an AppSec platform offers a unified security view across the entire SDLC, from code development to runtime. This ensures vulnerabilities are caught throughout the process, including container creation and deployment. Manual scans for individual containers are replaced by automated scans within the CI/CD pipeline, identifying and flagging issues early in development.

The vast number of container images creates a complex attack surface. A holistic AppSec platform, with vulnerability management, prioritizes threats based on severity and runtime exploitability. This allows teams to focus on the most critical issues first, optimizing remediation efforts. Like battlefield triage, a true platform provides a strategic view that allows you to direct resources to the most business-critical threats.

Enforcing consistent security policies crucial for your AppSec program. An AppSec platform offers a central location to define and enforce these policies for all applications. This ensures a consistency across all deployments, creating a unified security front.

When you utilize a container security solution that works within your application security platform, you will find that you have a much more centralized, automated, and holistic approach to AppSec. This translates to faster development, reduced security risks, and a stronger overall security posture.

A platform should be able to grow with you as your needs change over time. When comparing platform-based approaches, make sure they can correlate scan results across different scanning engines so you can obtain an overall risk assessment across projects and applications.

RECOMMENDATION

A true holistic AppSec platform provides a strategic view that allows you to direct resources to the most business-critical threats.

06

Developer Experience – No Longer an Option

Developers are constantly battling false positives and complex configurations. This frustration often leads to security workarounds, which can result in an increase in vulnerabilities being pushed into production. You must insert security into an existing work flow in order to get developers on board, and building containers is already part of a developer's workflow today. A DevEx-focused solution must seamlessly integrate into their existing workflows, and offer clear guidance without slowing them down.

The vast number of container images generates a constant stream of security alerts. Without clear prioritization, developers become overwhelmed, neglecting critical vulnerabilities. A solution that prioritizes threats based on severity and runtime exploitability empowers developers to focus on the most pressing issues. This translates to efficient remediation and a more secure application environment.

Traditionally, security has been separated from development. A DevEx-focused solution fosters collaboration. By providing in-context security feedback within the development environment, developers become active partners in achieving security goals. This improves trust morale, and strengthens the overall security posture of applications.

DevEx is no longer optional. Choosing a container security solution that prioritizes developer experience empowers them, streamlines development, and leads to more secure containerized applications. By focusing on DevEx, organizations can transform container security from a roadblock into a competitive advantage.

RECOMMENDATION

Prioritize developer experience to empower developers to make containerized applications more secure

Checkmarx Container Security

Checkmarx secures containers through a comprehensive suite of capabilities designed to identify and mitigate vulnerabilities at every layer of container images. Utilizing a multi-layered image scanning approach, Checkmarx analyzes base images, software dependencies, and application code to detect potential threats. This method ensures that vulnerabilities are identified early in the development process, minimizing security risks during deployment and operation.

→ Package inspection

Package inspection within container images is another critical capability of Checkmarx' container security solution. It verifies that packages adhere to security best practices, such as using the latest secure versions and ensuring proper licensing. This helps developers maintain compliance and avoid legal issues related to software usage.

→ Get the details

The ability to breakdown container images into granular details is pivotal for developers using Checkmarx. This capability allows them to drill down into each layer of an image, identifying specific vulnerabilities and package details. Armed with this detailed insight, developers can take targeted remediation actions, strengthening the overall security posture of their containerized applications.

→ Prioritize and act

Following vulnerability assessment, Checkmarx prioritizes identified issues based on severity and runtime data, ensuring that critical vulnerabilities are addressed promptly. This prioritization enables effective triage, allowing users to manage and track the status of vulnerabilities across projects or applications. Detailed remediation guidance is provided, empowering developers to implement necessary fixes and enhance the security posture of their containerized applications.

→ Comprehensive view

Checkmarx' results view interface provides comprehensive visibility into container security status. It offers a clear overview of vulnerabilities across various severity levels and allows users to analyze their distribution based on runtime status. This visibility aids in mitigation efforts and supports compliance assessments, enabling organizations to maintain security standards throughout their containerized environments.

Why Checkmarx

Checkmarx' container security is a comprehensive approach, combining multi-layered image scanning, package inspection, vulnerability assessment, triage, and remediation guidance. It provides vulnerabilities prioritization insights based on severity and runtime information. This enables proactive threat detection and mitigation. By integrating security throughout the development lifecycle, Checkmarx helps organizations effectively manage risks, maintain compliance, and protect against evolving cyber threats.

Experience the solution firsthand and see how it integrates seamlessly into your development workflow

Request a Demo ↗

Checkmarx

Checkmarx is the leader in application security and ensures that enterprises worldwide can secure their application development from code to cloud. Our consolidated platform and services address the needs of enterprises by improving security and reducing TCO, while simultaneously building trust between AppSec, developers, and CISOs. At Checkmarx, we believe it's not just about finding risk, but remediating it across the entire application footprint and software supply chain with one seamless process for all relevant stakeholders.

We are honored to serve more than 1,800 customers, which includes 40 percent of all Fortune 100 companies including Siemens, Airbus, Salesforce, Stellantis, Adidas, Walmart and Sanofi.