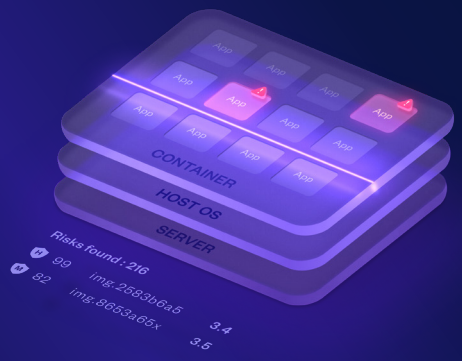
Checkmarx

Solution Brief

Container Security

Securing Containers Across
the Software Development Life Cycle



Key Challenges

Containerization has revolutionized software development by unlocking agility and speed. However, traditional security tools are struggling to keep pace. Unpatched vulnerabilities, misconfigurations, and hidden threats lurk within containers, jeopardizing your applications and data. Checkmarx offers a comprehensive solution designed to empower you in this new landscape.

- **Vulnerable Image Sources:** Public container registries can harbor malicious images, and inadvertent misconfigurations can expose sensitive information within images.
- **Volume of Alerts:** Overwhelming volume of alerts leads to alert fatigue and missed critical vulnerabilities.
- **Outdated Images and Dependencies:** Failure to keep container images and their dependencies up-to-date leaves them exposed to known vulnerabilities.
- **Static Scanning Limitations:** Traditional static scanning tools alone might miss emerging threats and misconfigurations, requiring insights and context from runtime.

Checkmarx Container Security

Checkmarx' container security solution tackles vulnerabilities across all image layers (base, code, dependencies) with up-to-date threat databases. It prioritizes exploitable risks, saving developers time by reducing noise by 90%. Actionable data (severity, secure base image options) empowers them to fix critical issues first. Integration with CI/CD pipelines ensures early detection, while our integration with Sysdig provides runtime insights for faster threat response. This comprehensive approach empowers secure container development and increased security posture.

How Does Checkmarx Container Security Work?

Checkmarx secures your containerized applications throughout their lifecycle. It scans container images, identifying vulnerabilities in base layers, code, and dependencies. Unlike basic scanners, Checkmarx prioritizes threats and offers remediation advice. It integrates with development workflows and provides runtime insights and context to detect, prioritize, and respond to threats. This comprehensive approach empowers developers to build secure containers and help security teams proactively manage container security.

Checkmarx Container Security Benefits

Noise Reduction

Cut through the day-to-day noise of AppSec tools with risk prioritization and runtime context.

Vulnerability Assessment

Prioritize vulnerabilities based on runtime exploitability and severity, with detailed information such as CVE details, potential impact, and remediation guidance.

Triage

Manage vulnerability severity and status per project. Update, verify, and track actions.

Remediation

Get recommendation for safer base images, and options for major/minor versions and alternatives all with clear impact on severity.

Results View

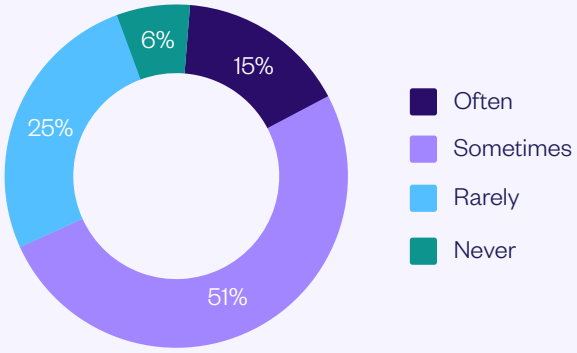
Pinpoint security risks (all severities, runtime status) for faster fixes.

Scan Risk Report

Generate comprehensive reports summarizing vulnerabilities and their severity for further analysis and compliance purposes.

Why Checkmarx Container Security?

Traditional security struggles with the complexity of containers. Checkmarx offers a multi-layered approach, analyzing all image parts (base, code, dependencies) for vulnerabilities with up-to-date databases. It prioritizes exploitable risks and empowers developers with detailed vulnerability information and remediation guidance (e.g., secure base images). Checkmarx integrates with CI/CD pipelines and Sysdig for runtime insights, enabling faster threat response. Granular image breakdown helps pinpoint issues, and actionable data streamlines the security process. Checkmarx goes beyond basic scanning, offering a holistic solution for secure containerized applications.



91% of organizations knowingly deployed vulnerable code into production

Key Features

Help your business better understand what to prioritize and fix, and why use Checkmarx Container Security

- **Image Scanning:** Checkmarx scans container layers (base, code, dependencies) for vulnerabilities and integrates with Sysdig to correlate runtime data, providing a holistic security view.
- **Image Breakdown:** Drill down into each layer of a container image to see vulnerabilities and package details. This allows developers to pinpoint security issues and take targeted remediation actions.
- **Vulnerability Assessment:** Prioritizes vulnerabilities based on runtime insights and risk. It also provides CVE details, potential impact, and remediation guidance.
- **Triage:** Manage the severity and status of vulnerabilities for each project or application. Update severity levels, change status (e.g., verify, not exploitable), and maintain detailed audit trails for all actions taken.
- **Remediation:** Identify vulnerabilities within container images and recommend alternative base images with a lower security risk profile. This helps developers choose more secure foundations for their applications.
- **Results View:** This interface provides a detailed view of container image scan results. Users can see the distribution of vulnerabilities across different severities and analyze them based on runtime status.
- **Scan Risk Report:** A comprehensive report summarizing scan results, including the number of vulnerabilities and their severity. These reports can be downloaded in various formats (JSON, CSV, PDF) for further analysis and compliance purposes.
- **Docker Extension:** Checkmarx scans container images within Docker workflows, giving developers real-time feedback on security risks. This helps them fix vulnerabilities early, improving container security.

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, Wal-Mart and Sanofi.