Application Security Posture Management

Make sense of AppSec data and fix what matters most.

Key Challenges

AppSec teams must manage separate tools that identify thousands of software vulnerabilities. Manually analyzing and correlating results across these different tools and interfaces makes it difficult to understand what's truly important, prioritize efforts, and triage for remediation.

↘ **Noise:** Too many vulnerabilities flagged by disparate point solutions leads to a flood of information and alerts

↘ **Correlation of Incompatible Data Sets:** Manual analysis and correlation is painful for AppSec teams, eating up valuable time and resources

↘ **Prioritization Paralysis:** Resources are limited, and it is difficult to know which vulnerabilities should actually be fixed

↘ **Communicating Progress to the Business:** Development cycles spent on security fixes are often seen as a diversion, and justification for the use of resources is difficult

↘ **Understanding Business Risk:** Solving the complex challenges above while reducing manual effort and maximizing business impact

Application Security Posture Management

The increasing pace of application development, the escalating complexity of applications, and the decentralization of teams responsible for both developing and securing applications have made application security incredibly challenging.

With a flood of data from multiple sources (of potentially varying quality), the effort to analyze, correlate, prioritize and triage application risk can be overwhelming. Checkmarx ASPM addresses these challenges, and gives you reliable visibility into, and control of, your application security posture from code to cloud to better manage risk.

How Does Checkmarx ASPM Work?

Checkmarx ASPM takes data from multiple application security testing (AST) tools, then correlates the results to provide guidance to AppSec teams on which vulnerabilities should be fixed first. In addition to pulling data from across the Checkmarx One platform, it also can ingest data via API from any tools capable of outputting AppSec testing data in the universal Static Analysis Results Interchange Format (SARIF).

Checkmarx ASPM gives you the power of Checkmarx' market leading AppSec solutions in concert with other solutions you may have, and the ability to correlate data, make sense of it, and prioritize your security efforts.

Checkmarx ASPM Benefits

Noise Reduction
Cut through the day-to-day noise of AppSec tools with targeted recommendations

Vulnerability Management
Make sense of vast amounts of vulnerability data from multiple sources

Triage
Reduce the manual effort of analysis and prioritization to help you understand what to do next

Measurement
Understand and demonstrate progress across your entire AppSec program

Understand Business Risk
Put vulnerabilities and remediation efforts in the context of what is critical to your business

Why Checkmarx ASPM?

Checkmarx is the leader in cloud native application security, and ASPM is the solution to the complexities of modern-day application security. ASPM helps AppSec teams analyze massive numbers of vulnerabilities, understand their overall posture, and make recommendations on which vulnerabilities to fix to make the largest reduction of risk possible for the business. It helps AppSec to strategically expand its efforts in alignment with overall enterprise risk, and communicate that risk in terms that other parts of the business can understand. ASPM helps AppSec teams to effectively scale their efforts surrounding the evaluation and mitigation of application security risk.

Your Application

Let's Remediate Your Riskiest Application

92
Critical

Remediate Application

⬇ Download Reports

Top 10 risky applications

Key Features

Help your business better understand what to fix and why with Checkmarx ASPM

↘ **Code to Cloud Visibility:** Automatically organize and view data across the entire application lifecycle, from development through runtime.

↘ **Comprehensive Coverage:** Monitor and correlate data across all your AppSec solutions, including Checkmarx and non-Checkmarx solutions

↘ **Orchestration of Checkmarx ASTs:** Integrate Checkmarx solutions from across the SDLC and manage their operation according to your organizational policies

↘ **Correlation:** Aggregate and correlate results from separate AppSec tools to reduce noise and better prioritize remediation efforts. This includes analysis of exploitable path, attack path, network exposure, and more

↘ **Cloud Insights:** Pulls data from cloud environments that can be correlated with our data from development to prioritize remediation

↘ **Application Risk Management:** Scores applications by risk and provides a single risk view of your entire application footprint, allowing you to focus remediation by application criticality or application risk

↘ **Bring Your Own Results:** Integrate findings from 3rd party tools via APIs

↘ **CNAPP Integrations:** Integrate with world-class partners, including Sysdig and Wiz, to correlate data from runtime environments

↘ **Executive Dashboard:** Track and measure AppSec KPIs in one dedicated location