CHECKMARX

CxIAST

Interactive Application Security Testing

Applications are the major attack vector when it comes to enterprise cyber-attacks. As awareness of the threat grows, more organizations realize that application security has many layers, including developer enablement, open-source assessment, static code analysis and dynamic (run-time testing) analysis.

CxIAST is an application security testing solution that detects vulnerabilities in running applications under test. By extending its portfolio into dynamic and continuous security testing, Checkmarx provides broader coverage, and improves time-to-market without compromising security.

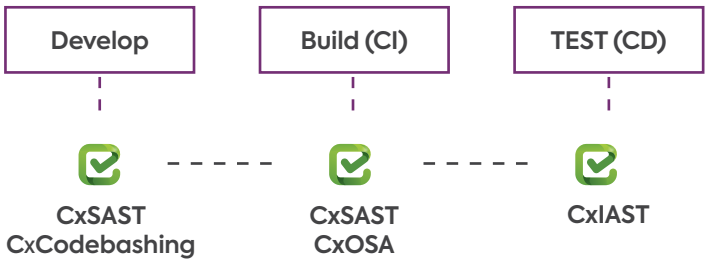
Security at the Speed of DevOps

CxIAST is purpose-built for DevOps and fits perfectly into your organization's CI/CD pipeline. It provides advanced vulnerability detection with zero impact on test cycle times, addressing the fast-paced software release timelines required today. An intelligent agent continuously monitors application behavior while CxIAST leverages existing functional testing tools to collect critical data points, and runs smart queries to detect security vulnerabilities. Resultant vulnerabilities are presented in an intuitive results dashboard to be assigned as security bugs and remediated.

- Global test automation market is being driven by rapid CI/CD adoption and estimated to be worth $85.8 billion by 2024 [1]
- Enterprise IAST adoption will have exceeded 30% by 2019 [2]

Complete Your AppSec Testing Portfolio

Legacy dynamic application security testing (DAST) solutions deploy as a Security Gate because long scan times delay production rollout. Now, with CxIAST continuous AppSec testing, delays are eliminated since vulnerabilities are detected in real-time. This fills a critical layer in your application security portfolio because certain vulnerabilities and flaws can only be detected on a running application. CxIAST is also simple to install, simple to operate and complements Checkmarx SAST, open source and developer enablement solutions.



Extends dynamic application security testing to multiple touch points across the SDLC

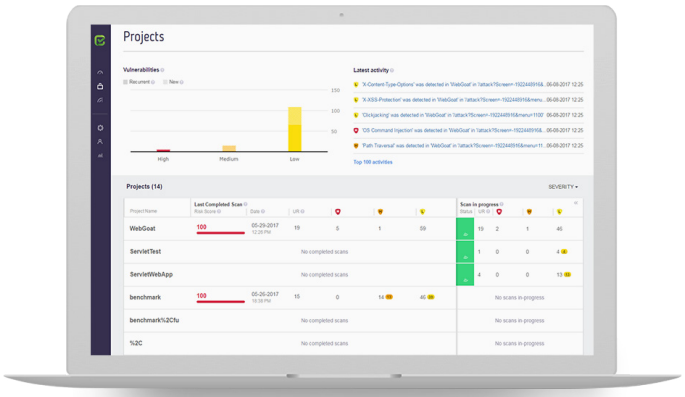
1: TMR, March 2016 2: Gartner Magic Quadrant, March 2017

How It Works

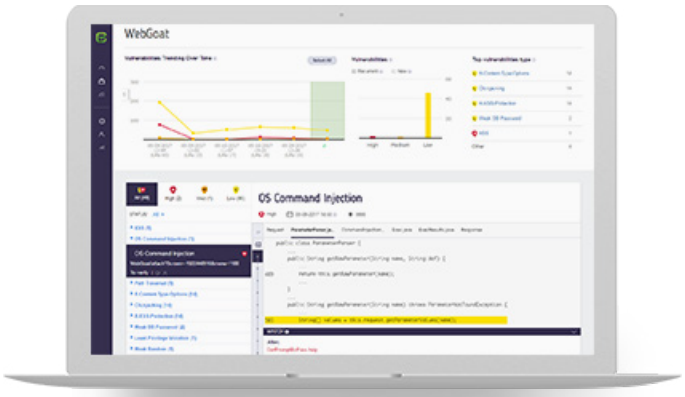
CxIAST has an agent that is customizable and instruments in-house functions unique to your organizational and compliance policies. The Checkmarx open query language allows you to modify existing security rules and even write your own. CxIAST identifies the full context for detecting vulnerabilities, and since data values pass through the running code, it can identify vulnerabilities quickly, accurately, and with minimum false positives.

CxIAST Key Benefits

- Improves time-to-market without compromising security
- Leverages dynamic application security testing for DevOps and CI/CD workflows
- Complements Checkmarx SAST, open source analysis, and developer enablement solutions
- Accurately monitors the behavior of applications and detects vulnerabilities in real-time, including OWASP Top Ten



Monitored Projects View



Application Dashboard

Vulnerability Coverage

CxIAST detects both input related and application vulnerabilities, including the OWASP Top Ten and more.

- SQL Injection
- XSS Injection
- OS Command Injection
- Path Traversal
- XPath Injection
- Parameter Tampering
- Open Redirect
- Trust Boundary Violation
- Cross-Site Request Forgery
- Decentralized RCE Vulnerability
- And more...

About Checkmarx

Checkmarx is the Software Exposure Platform for the enterprise. Over 1,400 organizations around the globe rely on Checkmarx to measure and manage software risk at the speed of DevOps. Checkmarx serves five of the world's top 10 software vendors, four of the top American banks, and many government organizations and Fortune 500 enterprises, including SAP, Samsung, and Salesforce.com. Learn more at Checkmarx.com or follow us on Twitter: @checkmarx.