CAST vs Checkmarx

Company Info

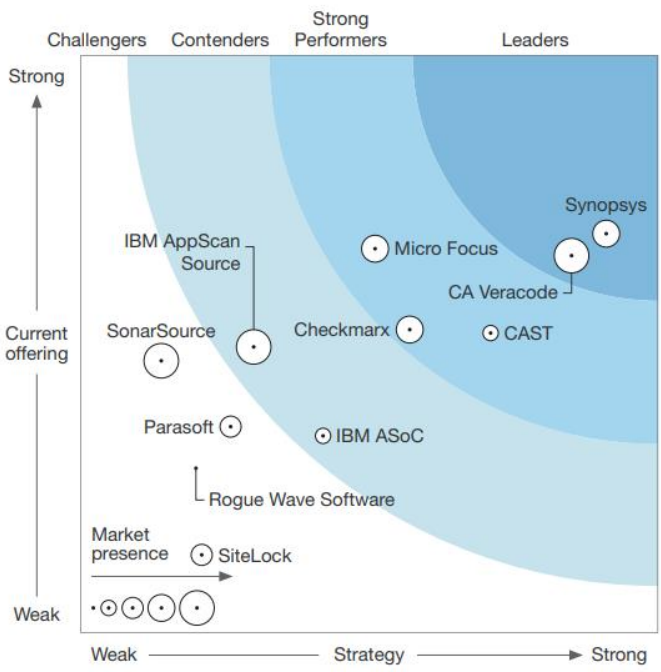
- Checkmarx was founded in 2006 and is headquartered In Israel.
- Focused on application security, Checkmarx has a SAST product and also provides Application Security Consulting as a service.

Customer Insights (Gartner Reports)

- Primary concern is the high level of false positives per analyst reports. The FP problem has also been validated by our existing customers.
- Customers feel the pricing scheme is not transparent and is arbitrary at times.

Summary

In the application security landscape, according to Forrester (2018 - the latest survey), CAST is stronger than Checkmarx both in terms of product strategy and the range of offering



- **Broader technology coverage:** CAST covers 50+ technologies, frameworks, and databases while Checkmarx is limited to 20+ - mostly modern languages.
- **System Level Analysis:** CAST's unique System Level Contextual Analysis understands the structure of the application and uses that intelligence to weed out the findings that are irrelevant, thereby reducing False Positives.
- **Extend Security**: We extend Security to the broader notion of resilience - the ability to prevent outages, data corruption, etc. CAST identifies structural issues and how those risks propagate through the software.
- **Insider Threats:** All pure application security players focus on the walls and doors(CWE, OWASP) to secure the applications. We do the same but in addition we also address insider threats (example : An unhappy employee or contractor coding a back door to the system).

Range of offering

	Application Security Toolkit		
	SAST – Static Application Security Testing	DAST –Dynamic Application Security Testing	Software Composition Analysis
CAST			
Checkmarx		Through Partners	

CAST does not offer Dynamic Analysis since our focus is on Shift-Left to intercept the flaws before they reach production.

Detailed Comparison

Feature	Checkmarx	CAST AIP
CWE Top-25	✓	✓
OWASP Top-10	✓	✓
CISQ Coverage	×	✓
Open Source Risk (including Proven CVE)	×	✓
Blueprinting for Insider Threat detection	×	✓
Extended Security(Resiliency) – Exception Handling, Memory Management etc.	×	✓
Architecture Rules & Compliance Monitor	×	✓
Cross-technology Transaction Mapping & Risk Measurement	×	✓
IDE Integration	✓	×
DevOps Tool Integration	✓	✓
Tagging Sensitive Data	×	✓