CAST MRI for Software vs Microfocus Fortify

(SAST)

Company Info

- Fortify was founded in 2003 and acquired by HPE in 2010.
- The software assets of HPE were merged with Microfocus in 2017, resulting in the current set up.
- Microfocus is a large ISV with ~250 enterprise products not limited to application security.

Summary

Fortify (SAST) is focusing on a few technologies where they can integrate their tools into the developers IDE. They are supporting 27 languages and their frameworks. Fortify can be deployed on-premise or as a service (Fortify on Demand). Pricing is per user, whatever the application size or technology coverage.

Main differences with CAST MRI for Software:

- **Broader technology coverage:** 100+ technologies, frameworks, and databases. Fortify supports PL/SQL and T-SQL.

- **System Level Analysis:** CAST performs automatic, full-system analysis of all data structures, code components, and reverse engineers all their interdependencies. 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 (see OWASP, Juliet benchmarks for superior, best-in-class False Positive rates).

- **Extend Security**: CAST extend Security to the broader notion of resilience - the ability to prevent outages, data corruption, etc. CAST tracks manipulation and access to data all the way from user entry to the database.

- **Architecture Studio:** CAST analyzes the architecture of applications and provides architecture adherence checks to intercept faulty constructions leading to security flaws as well as blocking performance issues. CAST Architecture Studio provides capabilities to define custom checks for home-made and custom frameworks.

- **Application Blueprints:** CAST Imaging provides interactive blueprints of the actual architecture of applications for teams to understand and visualize in real time its adherence with the intended TO-BE design, and its effects on the structural quality of the software system.

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

Detailed Comparison

Feature	Fortify	CAST MRI
CWE Top-25	✓	✓
OWASP Top-10	✓	✓
PCI DSS	✓	✓
ISO 5055 Coverage	×	✓
Blueprinting for Architecture Compliance	×	✓
Extended Security(Resiliency) – Exception Handling, Memory Management etc.	×	✓
Custom Framework Compliance Monitor	×	✓
Cross-technology Transaction Mapping & Risk Measurement	×	✓
IDE Integration	✓	×
DevOps Tool Integration	✓	✓