

CAST Vs Veracode - General

	Application Security Toolkit		
	SAST – Static Application Security Testing	DAST – Dynamic Application Security Testing	Software Composition Analysis
CAST	✓		✓
Veracode	✓	✓	✓

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

Detailed Comparison

Feature	Veracode	CAST AIP
CWE Top-25	✓	✓
OWASP Top-10	✓	✓
CISQ Coverage	✗	✓
Dynamic Analysis	✓	✗
Open Source Risk	✓	✓
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	✗	✓

CAST Highlight Vs Veracode – Software Composition Analysis



VERACODE

Functionality	CAST Highlight	Veracode SCA	Comments
Vulnerability Tracking	✓	✓	The capabilities are similar across the two products.
Portfolio-level OSS metrics	✓	✗	CAST HL provides the ability to roll up insights across a portfolio of applications enabling better management visibility and centralized management for teams that require this such as legal teams.
License Risk Management	✓ ✓	✓	CAST HL has sophisticated capabilities for tracking and managing license risk, copyright detection, license compatibility, license rulebooks, and more. Veracode SCA's license capabilities are limited.
Customizable Policies	✓ ✓	✓	HL offers customizable license policies. Veracode SCA's are limited.
Component reference database	✓	✓	CAST HL has 100+ million referenced third party components and 8+ billion unique file fingerprints.
Local Code Scan	✓	✗	CAST HL uses a local analyzer to scan code and does not require any code to be uploaded to SaaS portal. Veracode SCA requires code to be uploaded for analysis.
Software Bill of Materials	✓	✓	Both CAST HL and Veracode SCA provide SBOMs. CAST HL provides SBOMs in multiple formats – Excel, PPT, Word, JSON, CycloneDX, etc.
Transitive Dependencies	✓	✓ ✓	CAST HL reports transitive dependencies. Veracode SCA has reporting that goes multiple levels deep.
CI/CD Integration	✓	✓	Integrations with GitHub, BitBucket, Jenkins are available with CAST HL.
IDE Plugin	✗	✓	CAST HL CLI can be configured to integrate with dev tools for automation. Veracode SCA has an OOB IDE plugin.
Portfolio Advisor with OS Safety Index	✓	✗	CAST HL assesses OS risks across 100s of applications rapidly and provides automated recommendations.
Business Impact Data	✓	✗	CAST HL enables prioritization of OSS risks based on Business Impact, App Category, etc.
Browser Extension	✓	✗	CAST HL offers a free Chrome browser extension to deliver real-time insights while browsing web sites.
Pricing	\$	\$\$	CAST HL is priced based on application portfolio size (number of applications) with unlimited scans and unlimited number of users. Veracode SCA is more expensive.