







How is CAST Highlight different?

CAST is a unique comprehensive solution for [Software Composition Analysis](#), [Cloud Optimization](#), & [Application Portfolio Governance](#).

Capability	CAST Value	CAST differentiation with other products in the ecosystem	
Software Composition Analysis	<ul style="list-style-type: none">✓ Check 3rd party vulnerabilities✓ Control open source license compliance✓ Reduce Technology obsolescence✓ Comprehensive SBOMs in multiple formats	<div> Provides Management and Developer Level insights into OSS risks</div>	<div> Traditional SCA tools such as Sonatype are developer focused*</div>
Cloud Readiness & Optimization	<ul style="list-style-type: none">✓ Automatically segment applications for migration and modernization planning✓ Identify cloud native Blockers and effort to remove✓ Get cloud native service recommendations	<div> Fully automated, support for AWS, Azure, Google Cloud, IBM Cloud, VMWare Tanzu</div>	Not available in Sonatype
Application Portfolio Governance	<ul style="list-style-type: none">✓ Inventory application tech stack for baselining✓ Segment and Prioritize applications by Health & Business Impact✓ Enable Portfolio Rationalization & Tech Due Diligence for M&A✓ Gain insights on custom code: Resiliency, Agility, Technical Debt✓ Measure Green Impact and identify opportunities to improve sustainability	<div> Fully automated rapid insights across of 100s of applications in a week</div>	Not available in Sonatype

 provides a high  owing to multiple use cases.

* Detailed SCA comparison on next slide



Functionality	CAST Highlight	Sonatype	Comments
License, CVE, Obsolescence Tracking	✓	✓	The capabilities are similar across the two products and they both use multiple sources for vulnerability data. CAST HL also includes a license rulebook to interpret license legal text automatically.
Portfolio-level OSS metrics	✓	✗	CAST HL provides the ability to roll up insights across a portfolio of applications enabling better management visibility.
Software Bill of Materials (see more details on next page)	✓ ✓	✓	Both CAST HL and Sonatype provide SBOMs. CAST HL provides SBOMs in multiple formats – Excel, PPT, Word, JSON, CycloneDX, etc. CAST HL can also import existing SBOMs produced externally and update them with the latest insights on CVEs, licenses, etc.
Customizable Policies	✓	✓ ✓	Both products can be configured based on the corporate policies, deployment patterns, etc.
Component reference database	✓	✓	CAST HL has 100+ million referenced third party components and 8+ billion unique file fingerprints.
Contextual Analysis	✗	✓	CAST HL does not currently offer this. It is possible with CAST Imaging.
Emerging Vulnerabilities	✓	✗	CAST HL reports on CWEs in popular OSS components not yet reported in NVD via proprietary OSSIDB.
Transitive Dependencies	✓	✓ ✓	CAST HL reports transitive dependencies. Sonatype has reporting that goes multiple levels deep.
CI/CD Integration	✓	✓	Integrations with GitHub, BitBucket, Jenkins are available with both products.
IDE and Browser Extensions	✓	✓ ✓	CAST HL has a native extension for VS Code IDE and a browser extension. The CAST HL CLI can be configured to integrate with most dev tools for automation. Sonatype has several OOB IDE plugins.
Portfolio Advisor with OS Safety Index	✓	✗	CAST HL assesses OS risks across 1000s of applications rapidly and provides automated recommendations on priority actions.
Business Impact Data	✓	✗	CAST HL enables prioritization of OSS risks based on Business Impact, App Category, etc.
Container Scanning	✓	✓	The capabilities are similar across the two products.
Proprietary Component Governance	✓	?	CAST HL automatically detects proprietary and commercial components referenced in dependency files across the entire portfolio of applications. Users can then tag them, add documentation, and set policies.
Pricing	\$	\$\$\$	CAST HL is priced based on application portfolio size (number of applications) with unlimited scans and unlimited number of users. Sonatype charges per developer or per project and is typically much more expensive for similar sized implementations.

CAST Highlight SBOM Details

SBOM Feature	Description	Available in Sonatype and Most Traditional SCA Products
Component Details	Name of the open source or 3 rd party component as it is referenced in the CAST Highlight SCA knowledgebase, URL to origin of the component, the version number of the component, the date the version of the component was released	Yes
Common Vulnerabilities & Exposures (CVEs)	Security vulnerabilities reported in the National Vulnerability Database (NVD) for the given component version including the severity level (Critical, High, Medium, Low)	Yes
License	The open source license (if defined) for the version of the component along with a suggested risk level (High, Medium, Low)	Yes
Transitive Dependencies	Components that are indirectly referenced by a component as a transitive dependency	Yes
Component tags	Tag data pulled from the repository where the component lives (Github, maven, etc.)	?
Component description	Component description pulled from the repository where the component lives (Github, maven, etc.)	?
Export Formats	CAST Highlight supports multiple export formats for various audiences including: Excel (technical, security teams), Word (Legal teams), PPT, XML, CycloneDX.	Typically CycloneDX only
Gitlab Community Advisories	Security vulnerabilities reported via the Gitlab community.	No
Common Weakness Enumerations (CWEs)	Weaknesses within the code of the component that often correlate to future CVEs that have not yet been reported officially in the NVD. These are identified by CAST's structural quality engine that is run against popular OSS components and logged in the proprietary Open Source Software Intelligence Database (OSSIDB) only available in CAST Highlight.	No
Safer Component Versions	Recommended component versions to upgrade an existing component to that are safer (e.g., with CVEs that have been fixed). CAST Highlight recommends a both "safer and closest" and "safest" version.	No
Component copyright information	Copyright information for the component	?
License change tag	Indicates if a component had license changes over its lifetime.	No
License Rulebook	A user-friendly interpretation of the legal text of the license that includes clear indication of what the license allows, does not allow, requires, and additional properties.	No
Associated programming language	Component programming language pulled from the repository where the component lives (Github, maven, etc.)	?
Component status	Status of the component as defined in CAST Highlight by the organization (Allow, Deny, etc.) This requires the user to have an active subscription to CAST Highlight.	?
SBOM Importing	CAST Highlight can import externally produced SBOMs and update them with the latest insights.	?

Why CAST Highlight for SCA?

Business Value	Rationale	Benefits	Traditional SCA Products
Comprehensiveness	<ul style="list-style-type: none">• Broader insights go beyond open source risks to also include: software health, cloud readiness, green impact, software maintenance costs, and more• Portfolio-level views with automated roll-ups enable more comprehensive planning across 100s of applications and 1000s of OSS components• Exclusive Open Source Software Intelligence Database (OSSIDB) identifies weaknesses in popular OSS components representing possible future security vulnerabilities often weeks or months before reported by traditional SCA products	<ul style="list-style-type: none">• Ongoing insights for continuous optimization and modernization• Strong ROI on SCA investment• Stay ahead of emerging vulnerabilities before they become widely known or exploited	<ul style="list-style-type: none">• Focused OSS only• Focused on already known and reported vulnerabilities
Speed	<ul style="list-style-type: none">• Designed for rapid deployment, analyze 100s of applications in a few hours• Plugs directly into code repositories and automatically analyzes applications locally without code leaving the premises• SaaS based reporting dashboards provide insights with pre-defined and customizable views at both portfolio and individual application levels	<ul style="list-style-type: none">• Reduce deployment timelines• Improve time to value• Take action on risks quicker	<ul style="list-style-type: none">• Longer deployment times
Actionable Insights	<ul style="list-style-type: none">• Automated recommendations on specific actions to take and where to focus attention on most important applications to reduce open source risks (critical vulnerabilities and risky licenses)• Built-in surveys enhance code insights data with more contextual information (business impact, maintenance effort, etc.)• Portfolio level views with the ability to drill down into individual applications	<ul style="list-style-type: none">• Insights with business context• Identify and focus on the application priorities with the largest impact on the business first• Improve time to value	<ul style="list-style-type: none">• Developer-focused, tactical reporting• Harder to roll-up and get the portfolio-wide view• No contextual data
Pricing & Support	<ul style="list-style-type: none">• Priced based on the size of the application portfolio for unlimited users and regardless of application size• Global sales, services, and support teams with local offices in 9 countries	<ul style="list-style-type: none">• Lower cost• Higher ROI• Quicker response to support needs	<ul style="list-style-type: none">• 3x – 10x more expensive• No local presence in many countries