|  |  |
| --- | --- |
| Company | Synopsys Static Analysis – Formerly Coverity |
| Website | <https://www.synopsys.com/software-integrity/security-testing/static-analysis-sast.html> |

**The Bottom Line**

* Both Coverity and CAST Application Intelligence Platform (AIP) focus on identifying software defects and security vulnerabilities.
* Coverity is a static code analysis tool for developers while AIP is a solution that benefits developers, architects, product owners, and executive management.
* Both Coverity and AIP focuses on incorporating code quality and security into SDLC through automated code scan capabilities.
* Coverity excels at unit level static code analysis with incremental scan capability while AIP excels at contextual level static code analysis on contemporary languages, older languages, frameworks, middleware, ERPs, mainframe, etc.
* Coverity supports 14+ programming languages and scripts with emphasis on fast scan time achieved by fast desktop analysis.
* AIP supports 160+ technologies with emphasis on holistic software quality and risk measurements as well as comprehensive system analysis and understanding.
* Both Coverity and AIP offer public cloud, private cloud, and on-premise solutions.
* Coverity and AIP is an effective complementary solution to provide software quality assurance with Coverity as the developer’s tool in the IDE and AIP as the solution to ensure architecture integrity, conduct holistic analysis, and enable IT decision making with objective measurements.

|  |  |  |
| --- | --- | --- |
|  | Coverity | CAST AIP |
| Company Info | Privately held company founded in 2002 as an application defects detection technology provider. Focuses on incorporating software quality and security as part of software development process. Designed for developers and SDLC integration. Acquired by Synopsys in 2014. Coverity is now branded as ‘Synopsis Static Analysis’. Synopsis also offers dynamic testing, inside threat detection, thick client testing, and other testing technologies in addition to Coverity static analysis to complete its software security product solution. | Publicly traded company with 25+ years of experience in software quality analysis and measurement. USD $150M cumulative R&D investment. Provides system-level analysis to measure software quality, identify vulnerabilities, provide remediation advice, enforce architecture standard, produce application blueprint, and quantify application size. Brings fact-based transparency into software asset management, application development, quality and risk management, and maintenance and sourcing management. |
| Product Description | Performs static code analysis, open source code analysis, and software defect detection using patented techniques and interprocedural analysis. Provides deep full-path coverage accuracy and quickly analyze large codebase. Supports 14+ programming languages and frameworks with emphasis on fast scan time achieved by incremental scanning ability and fast desktop analysis. Offers public cloud, private cloud, and on-premise solutions. An industry leader in C++ application analysis. | Performs system level static code analysis from the UI layer to data layer. Supports 50+ programming languages and 100+ frameworks. Other technologies covered include opensource and scripting languages, ERPs, middleware, and databases. Focuses on software quality measurement, risk analysis, system blueprinting, architecture governance, and application sizing through in-depth understating of component interdependencies, transaction pathways, data flows, and automated function point and enhancement point calculations. Analyzes applications built with new/old generation languages and ERPs. Offers public cloud, private cloud, and on-premise solutions. |
| Target User(s) | Developers | Developers, Architects, Product Owners, Executive Management and CIOs |
| Coverage | Analyzes source code and underlying frameworks. Provides full path coverage and tests every potential execution path. Utilizes patented techniques to ensure deep and accurate analysis. | Analyzes across tiers of complex applications from top to bottom – UI layer to data layer – at the source code level and measures adherence to architectural and coding standards. |
| Quality & Security Check Personalization | May create personalized security adherence policy and quality assurance policy using Coverity’s SDK. | May create personalized security adherence policy and quality assurance policy using AIP’s configuration and customization interface as well as SDK. |
| Compliance Standard Supported | ISO, OWASP, PCI, and MISRA. | ISO/IEC, CWE, SANS, OMG, OWASP, CISQ, PCI, GDPR, and IFPUG. |

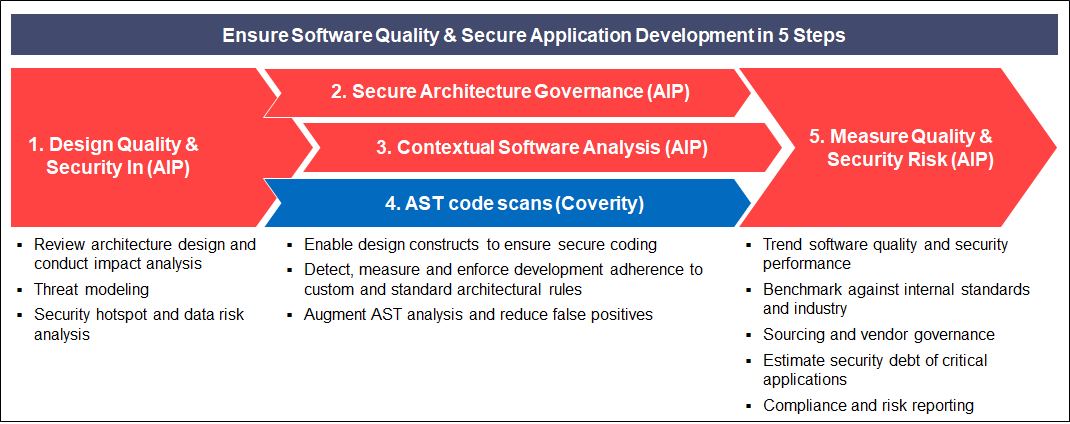
|  |  |  |
| --- | --- | --- |
|  | Coverity | CAST AIP |
| Analysis Output | Lists software vulnerabilities with degrees of criticality, defect locations, best fix locations, explanations and remediation advice. Reports on regulatory compliance for security and vertical markets requirements. | Lists vulnerabilities and violations with degrees of criticality, defect locations, best fix locations, explanations and remediation advice. Provides comprehensive system understanding and analysis including system blueprint, component interdependencies, architecture design, transaction pathways, and data flows. Produces measurements on Robustness, Complexity, Security, Efficiency, Reliability, Maintainability, Changeability, Transferability, Vulnerability Risk and other quality indicators. Uses industry standard - automated enhanced function point and automated enhancement point - to determine application size and productivity. |
| Characteristic & Attribute | Automated static and dynamic scan; Incremental scan; Parallel analysis; Fast desktop scan. Focused on software security and quality. Allows import of analysis results found by other analysis technologies. | Automated static contextual code analysis. Analyze security risk as well as other quality attributes such as Robustness, Complexity, Security, Efficiency, Reliability, Maintainability, Changeability, Transferability, and Vulnerability Risk. Allows import of analysis results found by other analysis technologies. |
| Key Integration | Integrates with IDE, build management servers, bug tracking tools, source repositories, application lifecycle management and reporting systems. | Integrates with build management servers, bug tracking tools, source repositories, reporting systems, automation and orchestration technologies. |
| Supported Language | 14+ technologies supported including programming languages and frameworks. A complete list of supporting technologies including Java, C#, .NET, PHP, Python, Android, C/C++, Node.JS, and Swift can be found at <https://www.synopsys.com/content/dam/synopsys/sig-assets/datasheets/SAST-Coverity-datasheet.pdf> | 160+ technologies supported including programming languages, opensource, scripts, frameworks, databases, interface languages, ERPs, mainframe, and middleware technologies used for enterprise application development. A complete list of supported technologies including Java, .NET, COBOL, C, C#, C++, iOS, PHP, HTML, JavaScript, PL/SQL, and SAP can be found at <http://doc.castsoftware.com/display/DOC82/Supported+Technologies>  <https://extend.castsoftware.com/V2/> |

|  |  |  |
| --- | --- | --- |
| Feature | Coverity | AIP |
| IDE Integration | ✓ | 🗶 |
| DevOps Tool Integration | ✓ | ✓ |
| Architecture Rules | 🗶 | ✓ |
| Customizable Data Flow | 🗶 | ✓ |
| Incremental Scan | ✓ | 🗶 |
| Cross-technology Transaction Mapping | 🗶 | ✓ |
| Propagation and Transaction Risk Measurement | 🗶 | ✓ |
| Tagging Sensitive Data | 🗶 | ✓ |
| Blueprinting | 🗶 | ✓ |

|  |  |  |
| --- | --- | --- |
| Feature | Coverity | AIP |
| CWE Top-25 | ✓ | ✓ |
| OWASP Top-10 | ✓ | ✓ |
| Input Validation (XSS, SQL Injection) | ✓ | ✓ |
| Customizable Quality and Security Rules | ✓ | ✓ |
| Memory Management | ✓ | ✓ |
| Exception Handling | ✓ | ✓ |
| Log Management | 🗶 | ✓ |
| Contextual System Analysis | 🗶 | ✓ |
| Import of Analysis Results Produced by Other Technologies | ✓ | ✓ |

|  |  |
| --- | --- |
| Coverity Advantage | CAST AIP Advantage |
| Coverity has smaller coverage of programming languages but offers incremental scan. It is attractive to environments where applications are developed using mainly contemporary languages. Coverity performs application code analysis and places importance on security.  An industry leader in C++ application analysis and memory management issue identification. | AIP has much broader set of supported technologies. It is attractive to environments where applications are developed using new/old generation languages, ERPs, and DBMS. AIP performs system level analysis and places importance on comprehensiveness – robustness, complexity, security, efficiency, reliability, maintainability, changeability, transferability, vulnerability risk. |

**CAST AIP Differentiation**



Coverity and AIP is an effective complementary solution to provide software quality assurance with Coverity as the developer’s tool in the IDE   
and AIP as the solution to ensure architecture integrity, conduct holistic analysis, and enable IT decision making with objective measurements.

|  |  |  |
| --- | --- | --- |
| Feature | Coverity | CAST Imaging |
| CWE Top-25 | ✓ | ✓ |
| OWASP Top-10 | ✓ | ✓ |
| Input Validation (XSS, SQL Injection) | ✓ | ✓ |
| Customizable Quality and Security Rules | ✓ | ✓ |
| Memory Management | ✓ | ✓ |
| Exception Handling | ✓ | ✓ |
| Log Management | 🗶 | ✓ |
| Contextual System Analysis | 🗶 | ✓ |
| Import of Analysis Results Produced by Other Technologies | ✓ | ✓ |
| IDE Integration | ✓ | 🗶 |
| DevOps Tool Integration | ✓ | ✓ |
| Architecture Rules | 🗶 | ✓ |
| Customizable Data Flow | 🗶 | ✓ |
| Incremental Scan | ✓ | 🗶 |
| Cross-technology Transaction Mapping | 🗶 | ✓ |
| Propagation and Transaction Risk Measurement | 🗶 | ✓ |
| Tagging Sensitive Data | 🗶 | ✓ |
| Blueprinting | 🗶 | ✓ |