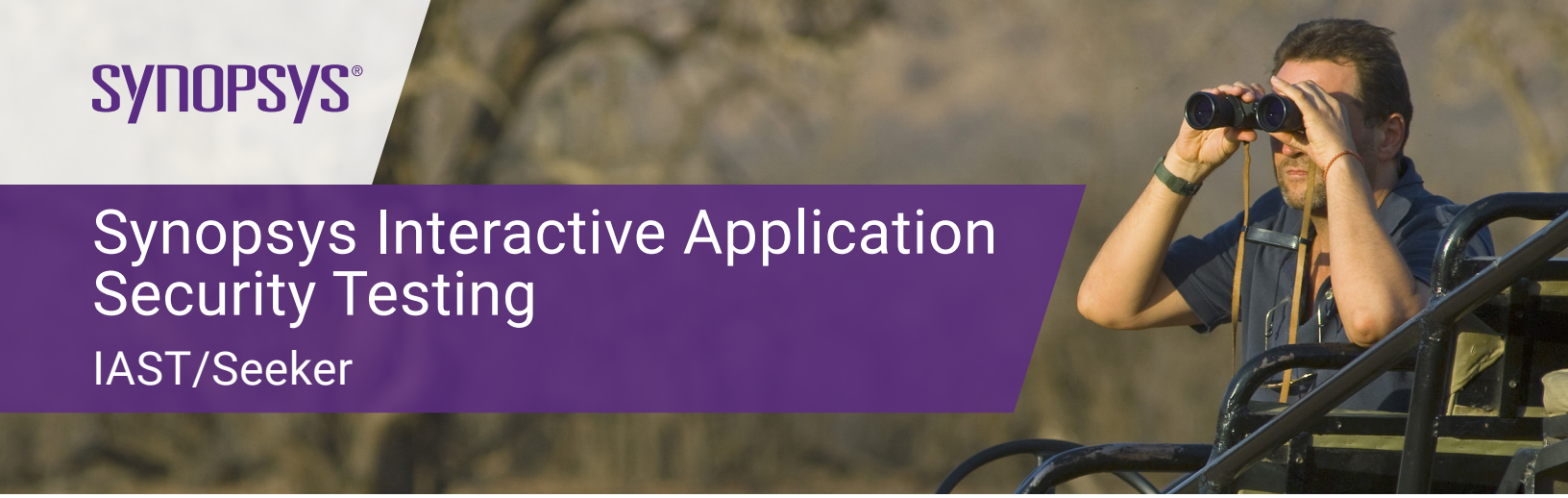
SYNOPSYS®



Synopsys Interactive Application Security Testing

IAST/Seeker

Automated and accurate identification of actual threats, seamlessly integrated into the SDLC

Synopsys Interactive Application Security Testing (IAST/Seeker) is leading the next generation of application security testing software. Easily integrating with your existing software testing processes, Synopsys IAST enables developers to develop secure applications efficiently.

Product overview

Synopsys IAST enables development teams to find verified security vulnerabilities across multitiered web applications and integrate runtime code analysis into the existing development life cycle. Our IAST solution accurately identifies real vulnerabilities that pose a threat to critical data, with full remediation guidance that enables developers to fix problems easily, even if they do not have security expertise.

Key features

Identifies real threats with accuracy

Our IAST tool's unique technology analyzes and correlates dataflow and runtime code execution. Synopsys IAST not only analyzes the code as it runs, line by line; it also examines the interaction of the code with your sensitive data across all application tiers and components. This technology can identify vulnerabilities that pose a real threat to critical data, including complex vulnerabilities and logical flaws no other technology can detect.

For even greater accuracy, Synopsys IAST simulates actual exploits on the application, thereby verifying results, minimizing false positives, and determining the impact and business risk of each vulnerability.

Provides clear, relevant results

Our "what you see is what you need to fix" approach minimizes false positives, ranks vulnerabilities by their impact, and provides only relevant results to developers. The results contain all the information necessary to fix the problem, including a clear explanation of the risk, a technical description, the vulnerable lines of code, and relevant, context-based remediation instructions. In addition, the tool's visual approach makes it easy to understand the problem and the risk.

Efficiently produce secure software

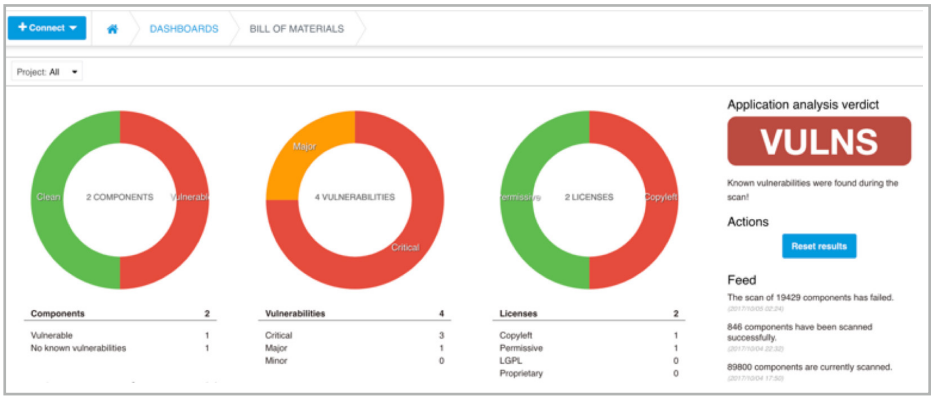
- Improve visibility into risk by understanding vulnerabilities in the context of business impact and exploitability.
- Don't waste time on nonissues. Synopsys IAST can verify identified vulnerabilities to ensure they are real and exploitable.
- Gain a clear view of the security status of your applications according to your compliance criteria.
- Enable developers to fix problems quickly, easily, and correctly by supplying all relevant context for every reported vulnerability.
- Improve your team's development and testing skills by teaching them how to develop secure code.

Easy to use and understand

Synopsys IAST brings simplicity to the software development life cycle (SDLC), delivering immediate results with little effort. The tool's innovative technology lies behind a simple, intuitive user interface that requires no security expertise to operate and allows users with no security background to run tests quickly and easily and receive focused, easy-to-understand results.

Optional SCA integration

Synopsys Software Composition Analysis (SCA/Protecode SC) can be used with Synopsys IAST to identify outdated libraries and security vulnerabilities in third-party and open source components. Reports for license types (e.g., GPL versus proprietary) and the number, type, and risk level (critical, major, or minor) of vulnerable components are available.



How it works

Identifies real business threats

- Synopsys IAST provides an accurate analysis of runtime code and dataflow in correlation with simulated attacks.
- False positives are greatly reduced.
- Our technology provides better, more accurate identification of all vulnerability types.
- Logical vulnerabilities are identified using the unique runtime code and dataflow correlation, which discovers vulnerabilities that other technologies and approaches can't.

Classifies risks and proposes solutions

- Synopsys IAST accurately assesses the impact and classifies the risk of each vulnerability through simulated exploits and data analysis.
- Detailed results include the vulnerable source code for each vulnerability.
- Focused, context-based remediation information allows developers to fix all vulnerabilities immediately, without prior security knowledge.
- Remediation instructions include a simple explanation of the fix and suggest secure code in the relevant programming language.

Integrates security into the development process

- Synopsys IAST doesn't require any manpower overhead or any knowledge of security or advanced technical skills.
- Our technology brings simplicity to the SDLC, delivers immediate results, and can be integrated with any development methodology.
- Accurate, clear, and simple, Synopsys IAST, the best-quality application security testing solution, maximizes your return on investment to secure your applications.

SYNOPSYS®

Synopsys Interactive Application Security Testing (IAST/Seeker) **Technical Specifications**

Supported languages

- C#
- Clojure (JVM, CLR)
- Groovy
- Java
- JavaScript (client)
- PHP
- PL/SQL
- Scala (incl. Lift)
- T-SQL
- VB.NET

Supported platforms

Languages/testing platforms

- .NET (2.0 or higher)
  - IIS
- Java
  - Any Java EE Server
  - GlassFish
  - JBoss
  - Tomcat
  - WebLogic
  - WebSphere
- PHP (5.2 or higher)
  - Apache
  - IIS
- PL/SQL
  - Oracle
- T-SQL
  - MS SQL Server

Runtime/frameworks

- .NET/CLR
  - ASP.NET MVC
  - Enterprise Library
  - Entity Framework
  - NHibernate
  - Ninject
  - NVelocity
  - OWASP ESAPI
  - SharePoint
  - Spring.NET
  - Telerik
  - Unity
- Java/JVM
  - Enterprise JavaBeans (EJB)
  - Grails
  - GWT
  - Hibernate
  - OWASP ESAPI
  - Play
  - Seam
  - Spring
  - Struts
  - Vaadin
  - Velocity
- PHP
  - CakePHP
  - CodeIgniter
  - Kohana
  - Laravel
  - OWASP ESAPI
  - Phalcon
  - Smarty
  - Symfony
  - Yii
  - Zend

Technologies

- Databases
  - DB2
  - HSQLDB
  - MongoDB
  - MS SQL
  - MySQL
  - Oracle
  - PostgreSQL
- Application types
  - Ajax
  - Google Web Toolkit (GWT)
  - JSON
  - Mobile (over HTTP)
  - RESTful
  - SOAP
  - Web (incl. HTML5)
  - Web services

SDLC integrations

Build/test or CI/CD

- Bamboo
- HP Quality Center
- IBM ClearCase
- Jenkins/Hudson
- MS Team Foundation Server
- TeamCity
- Other platforms via Seeker CLI or REST API

Testing frameworks

- Apache JMeter
- HP Quality Center
- IBM ClearCase
- Selenium
- Other frameworks via Seeker Proxy and CLI

Issue tracking

- Bugzilla
- HP Quality Center
- IBM ClearQuest
- Jira
- Mantis
- MS Team Foundation Server
- Rally / CA Agile
- Trac
- VersionOne

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in static analysis, software composition analysis, and application security testing, is uniquely positioned to apply best practices across proprietary code, open source, and the runtime environment. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations maximize security and quality in DevSecOps and throughout the software development life cycle.

For more information go to www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com

SYNOPSYS®
Silicon to Software™

03/23/18.DS_IASTSeekerV1_032318.