

Polaris Software Integrity Platform

An integrated, cloud-based AST solution optimized for modern DevSecOps

Polaris is an easy-to-use application security platform, optimized for modern DevSecOps, with the power and scalability enterprises need.

Overview

Polaris Software Integrity Platform® is an integrated, software-as-a-service (SaaS) application security platform powered by the industry's leading static application security testing (SAST), software composition analysis (SCA), and dynamic application security testing (DAST) engines. It provides fast, multitype scanning capabilities with highly accurate results triaged by Synopsys security experts. An easy-to-use and cost-effective solution that can scale with business application security needs, Polaris enables application security and development teams to collaborate in real time and meet release deadlines while managing enterprise application risk holistically.

Key benefits

- **Flexibility.** The on-demand, integrated AppSec platform makes it easy to provision, manage, and monitor enterprise-wide scanning and assessments 24x7.
- **Scalability.** Scale application security cost-effectively. Whether your organization requires testing for a single application or thousands, Polaris delivers a unified SaaS platform to meet your needs.
- **Ease of use.** Easy onboarding, deployment, and testing from a single unified platform. Seamless integration with existing developer, test automation, and CI/CD workflows.
- **Concurrent scanning.** Concurrent scanning improves performance by allowing you to run SAST, SCA, and DAST analysis at the same time. There is no limit to the number of tests you can run.
- **Accurate findings.** Synopsys market-leading SCA, SAST, and DAST engines provide complete and highly accurate results. Expert analysis and triage for SAST results is also available to further improve results by identifying and removing false positive findings.
- **Enterprise visibility.** Polaris dashboards and reports give you a view of vulnerabilities and trends across all your teams and applications.



Key features

fAST Static

Polaris fAST Static allows organizations to perform automated static analysis of all codebases, making it easy for developers and testers to find potential security flaws in their code early in the software development life cycle (SDLC).

The screenshot shows the Synopsys fAST Static interface for a project named 'insecure-bank'. The main view displays a table of detected issues:

Issue Type	Location	Filename/Origin	Tool Type	Triage Status	CWE	Vulnerability	Jira ID	First Detected
Cross-site Scripting	src/main/java/org/hdivsamples/controllers/DashboardController.java	DashboardController.java	SAST	Not Triaged	CWE-79			Oct 14, 20...
SQL Injection	src/main/java/org/hdivsamples/controllers/DashboardController.java	DashboardController.java	SAST	Not Triaged	CWE-89			Oct 14, 20...
SQL Injection	src/main/java/org/hdivsamples/controllers/DashboardController.java	DashboardController.java	SAST	Not Triaged	CWE-89			Oct 14, 20...
SQL Injection	src/main/java/org/hdivsamples/controllers/ActivityController.java	ActivityController.java	SAST	Not Triaged	CWE-89			Oct 14, 20...
SQL Injection	src/main/java/org/hdivsamples/controllers/DashboardController.java	DashboardController.java	SAST	Not Triaged	CWE-89			Oct 14, 20...

The 'Issue Details' section for a 'Cross-site Scripting' issue is expanded, showing the source code and remediation steps:

```
IOUtils.copy(file.getInputStream(), new FileOutputStream(tmpFile));
ObjectInputStream ois = new ObjectInputStream(file.getInputStream());
ois.readObject();
ois.close();
```

1. Reading data from an HTTP request, which is considered tainted.
2. Concatenating "file.getOriginalFilename()" to an HTML page allows cross-site scripting, because it was not properly sanitized for context HTML PCDATA block.
3. Perform the following escaping in the following order to guard against cross-site scripting attacks with Java. For example: "Encode.forHtml(file)" * Use the "Encode.forHtml" function from the OWASP Java Encoder. This escapes the output for HTML.
4. Printing to HTML output.

```
return "<p>file " + file.getOriginalFilename() + " uploaded successfully/</p>";
else {
    return "<p>file " + file.getOriginalFilename() + " not processed, only previously downloaded malicious file is allowed/</p>";
}
```

fAST SCA

Polaris fAST SCA allows organizations to automate software composition analysis across the SDLC, providing a complete Bill of Materials (BOM) of nonvulnerable and vulnerable open source components, including licenses used, dependency trees, and origins, as well as upgrade guidance.

The screenshot shows the Synopsys fAST SCA interface for a project named 'SIGApp > TestProject'. The main view displays a table of components:

Security Risk	Component Name	Match Type	Usage	License Name
Critical	Apache Ant 1.7.1	Transitive Dependency	Dynamically Linked	LGPL-2.1+
High	Apache Ant 1.7.1	Transitive Dependency, Direct Dependency, Files Modified		LGPL-2.1+
Low	Apache Ant 1.8.0	Transitive Dependency (x2)	Dynamically Linked	LGPL-2.1+
Medium	Beanshell-Client 1.4.6	Transitive Dependency	Dynamically Linked	LGPL-2.1+ (x1)
Low	FreeBSD/jar 2.0.1	Transitive Dependency	Dynamically Linked	Apache 2.0

The 'Component Details' section for 'Apache Ant 1.7.1' is expanded, showing:

- Component Description:** Apache Ant is a Java-based build tool. In theory, it is kind of like Make, but without Make's wrinkles.
- Component Links:** <https://github.com/akita-oka/commons-jars/akta-config-check>
- Component Origins:**
 - 1. apache:ant:ant-launcher:software-ant:1.7.1 (Upgrade Guidance Available)
 - 2. maven:org:ant:launcher:1.7.1 (No Upgrade Guidance)
- Current Vulnerabilities:** 10 Critical, 2 High, 2 Medium (10 Matches). View Dependency Tree.
- Upgrade Guidance:** Short Term Upgrade Recommendation: 1.7.2. Knows short term vulnerabilities: 1 High, 2 Medium. Long Term Upgrade Recommendation: 1.8.0. Has no known vulnerabilities.

The 'Dependency Tree' section shows a tree structure for 'Component Origin: maven:org:apache:ant:ant-launcher:1.7.1' with 10 matches, including Cargo Core Uberjar and Apache Ant 1.7.1.

FAST Dynamic

Polaris fAST Dynamic allows organizations to run quick, self-service DAST analysis of modern web applications without slowing development down. No complex configuration or setup required. Automate and scale testing of hundreds of websites easily with built-in settings to choose from.

The screenshot displays the Synopsys fAST Dynamic interface for a project named 'Insecure Shoppe'. The main view shows a table of 16 matching issues. The table columns include Issue Type, Location, Attack Target, Triage Status, CWE, Vulnerability ID, Fix-By, and First Detected. The issues listed are:

Issue Type	Location	Attack Target	Triage Status	CWE	Vulnerability ID	Fix-By	First Detected
Improper Neutralization of Special Elements used in SQL Co...	https://altorj.tinfoilsecurity.com/altorj/doLogin	uid	Not Triaged	CWE-89		in 5 days	Mar 19, 2024, 1:11 AM
Improper Control of Interaction Frequency	https://altorj.tinfoilsecurity.com		Not Triaged	CWE-770		in 12 days	Mar 19, 2024, 1:11 AM
Use of Web Browser Cache Containing Sensitive Information	https://altorj.tinfoilsecurity.com/admin/		Not Triaged	CWE-525		in 28 days	Mar 19, 2024, 1:11 AM
Exposed Dangerous Method or Function	https://altorj.tinfoilsecurity.com/doSubscribe	Method	Not Triaged	CWE-749		in 28 days	Mar 19, 2024, 1:11 AM
Inadequate Encryption Strength	https://altorj.tinfoilsecurity.com/altorj/feedback.jsp	[TLS_ECDHE_RSA_WITH...	Not Triaged	CWE-326		in 28 days	Mar 19, 2024, 1:11 AM
Insufficient Verification of Data Authenticity	https://altorj.tinfoilsecurity.com/altorj/util/serverStatus...	HostName	Not Triaged	CWE-345		in 28 days	Mar 19, 2024, 1:11 AM
Cross Site Scripting - Reflected	https://altorj.tinfoilsecurity.com/altorj/util/serverStatus...	HostName	Not Triaged	CWE-79		in 28 days	Mar 19, 2024, 1:11 AM

The detailed view for the 'Cross Site Scripting - Reflected' issue shows the following information:

- Location:** https://altorj.tinfoilsecurity.com/altorj/util/serverStatusCheckService.jsp?HostName=<script>alert(985510345);</script>
- Issue Details:**
 - First Detected:** Mar 19, 2024, 1:11 AM
 - Fix-By:** in 28 days (Apr 18, 2024, 1:11 AM)
 - Issue Type:** Cross Site Scripting - Reflected
 - Description:** Reflected XSS (Non-Persistent) occurs when an injection from one request is displayed in a following response from the web server.
- Tool:** fAST-DAST
- Scan Date and Time:** Mar 20, 2024, 9:29 AM
- Vulnerability: Overall Score:** 6.1
- Severity:** Medium

Expert verification and analysis

SAST scan results are reviewed with false positives removed, and critical findings prioritized for timely remediation.

AI-enabled remediation guidance

AI-driven remediation assistance that provides concise, developer-friendly descriptions with risk information alongside specific code fix recommendations, powered by Polaris Assist.

Seamless integrations

The easy-to-use platform provides seamless integrations with development and DevOps toolchains.

Policy management

Customizable rules can be set up in minutes per defined business risk policy.

Enterprise insights

Get organization-wide insights into the overall health and effective risk posture across apps and projects.

Choose the Polaris offering best suited to your needs

Feature	Description	Polaris SAST Subscription	Polaris SCA Subscription	Polaris DAST Subscription	Polaris Package SCA/SAST
fAST Static	Automate static analysis across the SDLC	●			●
fAST SCA	Automate software composition analysis across the SDLC		●		●
fAST Dynamic	Self-serve, automated dynamic web application testing			●	
Expert triage option	SAST analysis results are reviewed by Synopsys security experts to assist with prioritization and false positive removal	●			●
SCM integrations	Quickly onboard applications directly from your repositories	●	●		●
Policy management	Simplify policy management through optimized rules, automating enforcement of security and risk policies	●	●	●	●
Concurrent scanning	Run multiple types of scans on target application simultaneously	●	●	●	●
CI/CD integrations	Automate application security in DevOps pipelines	●	●	●	●
Flexible reports, analytics	Manage risk, measure, and improve your risk posture using enterprise analytics capabilities	●	●	●	●

Language and package manager support

SAST languages

- Salesforce Apex
- C/C++
- C#
- DART
- Go
- Java
- JavaScript
- Kotlin
- Objective-C/C++
- PHP
- Python
- Ruby
- Swift
- TypeScript
- Visual Basic

IaC platforms and formats

- AWS Cloud Formation
- Kubernetes
- Terraform
- YAML
- JSON

SCA package manager support

- XML
- Apache Ivy
- BitBake
- Cargo
- Carthage
- CocoaPods
- Conan
- Conda
- CPAN
- CRAN
- Dart
- Erlang/Hex/Rebar
- Git
- Go Dep
- Gogradle
- Go Modules
- Go Vendor
- Gradle
- Hex
- Lerna
- Maven
- npm
- NuGet
- Packagist
- PEAR
- pip
- pnpm
- Poetry
- RubyGems
- SBT
- Swift and Xcode
- Yarn

Source code management (SCM) system support

- GitHub
- GitLab
- Azure DevOps
- Bitbucket

The Synopsys difference

Synopsys provides integrated solutions that transform the way you build and deliver software, accelerating innovation while addressing business risk. With Synopsys, your developers can secure code as fast as they write it. Your development and DevSecOps teams can automate testing within development pipelines without compromising velocity. And your security teams can proactively manage risk and focus remediation efforts on what matters most to your organization. Our unmatched expertise helps you plan and execute any security initiative. Only Synopsys offers everything you need to build trust in your software.

For more information about the Synopsys Software Integrity Group, visit us online at www.synopsys.com/software.

©2024 Synopsys, Inc. All rights reserved. Synopsys is a trademark of Synopsys, Inc. in the United States and other countries. A list of Synopsys trademarks is available at www.synopsys.com/copyright.html. All other names mentioned herein are trademarks or registered trademarks of their respective owners. April 2024.