Polaris Software Integrity Platform

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

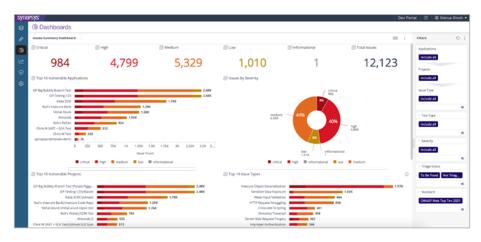
Polaris is an easy-touse application security platform, optimized for modern DevSecOps, with the power and scalability enterprises need.

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).

nor	PSYS:									Der	r Portal 🔿 🧃		
8	lisecure-bank → 🏵 insecure-bank / 🖇 main (default)												
>	Summary Issues Components Licenses Tests Branches Settings												
2	Clear Filters (2)				PREV N		Displaying 100 out of 104 matching issues Triage All 104 Export All 1						
	 Triage Status 		Ŧ	Issue Type 🐨	Location -	Filename/Origin 👻	Tool Type 👻	Triage Status	CWE -	Vulnerability Jira	ID 👻 First Dete		
,	 Issue Type 		н	Cross-site Scripting	src/main/java/org/hdivsamples/controllers/DashboardController.java	DashboardController.java	SAST	Not Triaged	CWE-79		Oct 14, 20		
	 Issue Category 		H	SQL Injection	src/main/java/org/hdivsamples/controllers/DashboardController.java	DashboardController.java	SAST	Not Triaged	CWE-89		Oct 14, 20		
	 Severity 		н	SQL Injection	src/main/java/org/hdivsamples/controllers/DashboardController.java	DashboardController.java	SAST	Not Triaged	CWE-89		Oct 14, 20		
	 Tool Type 2 SAST (104) SCA (303) 		н	SQL Injection	src/main/java/org/hdivsamples/controllers/ActivityController.java	ActivityController.java	SAST	Not Triaged	CWE-89		Oct 14, 20		
			н	SQL Injection	src/main/java/org/hdivsamples/controllers/DashboardController.java	DashboardController.java	SAST	Not Triaged	CWE-89		Oct 14, 20		
	Location	Issue Details Contributing Code Events											
	▶ CWE					2	_						
	 Standard 	Severity: 🔟 Issue Type: Cross-site Scripting 2 occurrences PREV NEX											
	 Owner 	Location: src/main/java/org/hdivsamples/controllers/Dashboard/Controller.java											
<pre>IOU:lls.copy(file.getToputTream(), new FileOutputStream(tmpFile)); ObjectToputTream Oils = new ObjectInputStream(file.getInputStream()); Oils.readObject(); Oils.close();</pre>													
		1. Reading data from an HTTP request, which is considered tainted.											
2. Concatenating "Hie getOriginalFilename()" to an HTML page allows cross-site scripting, because it was not properly sentized for context HTML PCDATA block.													
		E			to guard against cross-site scripting attacks with Java. For example: "Encode forHtm	sl(file)" * Use the "Encode.forHtml	" function from the	e OWASP Java Enco	der. This escap	es the output for HTML.			
		4. Printing to HTML output. return "File '" + file.getOriginalFilename() + '' uploaded successfully";											
		else											

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.

summary Issues	Component	Licenses	Tests Settings									
iters	8 🔽	PRIV NOT 2,021 results scress 30 pages							→ Export Bill of Materials	\otimes		
omponent v			✓ Match Type ▼	Usage +	License Name *		2 components selected across 1 page					
Search by Name						LGPL-2.1+						
Apache Ant (3)		-	Apache Ant 1.7.1	Transitive Dependency	Dynamically Linked				File Type			
Apache Log4j (1) Beanshell (1)		High	Apache Ant 1.7.1	Transitive Dependency, Direct Dep	pendency, Files Modified	LGPL-2.1+			 SPDX - json CycloneDX - json 			
BeanstalkClient (1)	0	Low	Apache Ant 1.8.0	Transitive Dependency (+2)	Dynamically Linked	LGPL-2.1+						
 FindBags jsr (1) javadiff-stills (1) 		Medium	BeanstalkClient 1.4.6	Transitive Dependency	Dynamically Linked	LGPL-2.1+ (+1)			File Name (Optional)			
JavaCV (1)		Low	FindBuos isr 2.0.1	Transitive Dependency	Dynamically Linked	Apache-2.0			Add Filename			
License 👻									Export 2 Components			
Search by Name	Cor	nponent Details	Security Details Licenses						Expert 2 Components			
Apache 2.0 (2)	Seco	Security Risk: 🛄 Component Name: Apucho Ant 1.7.1							Dependency Tree			
 Acme License (3) CCLicense (2) 	1.7							Component Origin: maven: org.apache.ant.art-launcher:1.7.1				
Google VP8 (3)	Ары		based build tool. In theory, it is kind of		Component Origins:							
Jabber Open Source (2)		Aake, but without	Make's wrinkles.	apache.ant:ant-las	Lepache.ant.ant-launcher-software-ant.1.7.1 Opprofe Existence Available mayee: org.ant-launcher:1.7.1			(10 matches)				
LaTeX Public License(1) MPL-2.0 (2)		ponent Links: //github.com/ok	ta/okta-commons-java/okta-config-che	🚖 Upgrade Guidance Au				com.synog com.syno	psys.sig:norby:2021 1029-SNAPSHOT psys.sig:norby:2021 1029-SNAPSHOT			
Public Domain (9)									go Core Uberjar 1.2.0			
Simple Search License(1)				No Upgrade Guidance		EE View Dependency	Tree		over, org.codehaus.corpo.corgo-core-oberjar.1.2.0			
ZShell(2)						Upgrade Guidance: Short Term Upgrade Re	commentation		lpache Ant 1.7.1 maren: org.apache.ant.ant-launcher.1.7.1			
Match Type 💌						1.7.2		go Core Uberjar				
 Transitive Dependency (27) Direct Dependency (20) 						Known short term vuln	rabilities		over: erg-codehaus.cargo.cargo-core.ubeijac12.0			
Files Modified (4)						Long Term Upgrade Re	onmendation .		Ipache Ant 1.7.1 maves: org.apache.ant.ant.launcher.1.7.1			
Files Added/Deleted (3)												
Security Risk 💌							Has no known vulnerabilities	com.synopsys.sig.norby:2021 1029-SNAPSH0T com.synopsys.sig.norby:2021 1029-SNAPSH0T				
Critical (21)							- [corn.		com. synopsys. sig:norby:2021 1029-SNAPSHOT			
Medium (212)								com synop	pays sig norby 2021 1026 SNAPSHOT			
🖸 Low (676)								com.synop	psys.sig.norby:2021 1029-SNAPSHOT psys.sig.norby:2021 1029-SNAPSHOT			
									psys.sig:norby:2021 1029-SNAPSHOT			

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.

synor Se		secure Shoppe > 🍄 project6						Dev Port	al 🕜 🕲 greg patton 🕶				
ð	Issues Tests O Settings												
Ø	•				Displaying 16 out of 16 matching is								
¢	•	Issue Type 📼	Attack Target 👻	Triage Status 👳	CWE 👳	Vulnerability ID 👳	Fix-By 👳	First Detected 👳					
	C	Improper Neutralization of Special Elements used in SQL Co	https://altoroj.tinfoilsecurity.com/altoroj/dol.ogin	uid	Not Triaged	-		in 5 days	Mar 19, 2024, 1:11 AM				
		Improper Control of Interaction Frequency	https://altoroj.tinfoilsecurity.com		Not Triaged			in 12 days	Mar 19, 2024, 1:11 AM				
	Use of Web Browser Cache Containing Sensitive Information		https://altoroj.tinfoilsecurity.com/admin/		Not Triaged	CWE-525		in 28 days	Mar 19, 2024, 1:11 AM				
		Exposed Dangerous Method or Function	https://altoroj.tinfoilsecurity.com/doSubscribe	Method	Not Triaged	CWE-749		in 28 days	Mar 19, 2024, 1:11 AM				
	•	Inadequate Encryption Strength	https://altoroj.tinfoilsecurity.com/altoroj/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://altoroj.tinfoilsecurity.com/altoroj/util/serverStatus	HostName	Not Triaged CWE-345			in 28 days	Mar 19, 2024, 1:11 AM				
	0 м	Cross Site Scripting - Reflected	HostName	Not Triaged	in 28 days	Mar 19, 2024, 1:11 AM							
	Issue D	Details Evidence		—					8				
	Location	n: https://altoroj.tinfoilsecurity.com/altoroj/util/serverStatusCheck	Service.jsp?HostName= <script>alert(985510345);</script>						Hide File Path				
	Issue	Details											
		Detected:		Tool:									
		9, 2024, 1:11 AM		fAST-DAST									
	Fix-By in 28 d	r: Jays (Apr 18, 2024, 1:11 AM)			Scan Date and Time: Mar 20, 2024, 9:29 AM Vulnerability: Overall Score 6.1								
	Issue	Type:		Vulnerability: Over									
		Site Scripting - Reflected											
		iption: ted XSS (Non-Persistent) occurs when an injection from one requ	Severity: Medium										

Expert verification and analysis

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

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	•	•	٠	•
Concurrent scanning	Run multiple types of scans on target application simultaneously	•	•	٠	•
CI/CD integrations	Automate application security in DevOps pipelines	•	•	٠	•
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

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.

Source code management (SCM) system support

- GitHub
- GitLab
- Azure DevOps
- Bitbucket