SCANTIST SCA SCANTIST PRODUCT SPECIFICATION

Thompson is Scantist's Software Composition Analysis tool designed to help you manage security and legal-compliance risks of your open source libraries in your source-code and binary projects so you:

Know which open source libraries you are using

Know which libraries are vulnerable

Know which libraries are compliant







Enhanced Visibility

- Complete open source Software Bill-of-Materials as part of your overall software supply chain to identify vulnerable and non-vulnerabilities components
- Direct and transitive dependency analysis detailed in the **Dependency Graph**
- Organisation-wide dependency mapping allows to identify and prioritise vulnerabilities using Knowledge Graph
- Curated reports in a variety of formats for management and/or integration
- Secure no access to source code

Managing Compliance to Licensing terms

- Scalable OSS Governance using customised policy rules as per your organisations needs
- Policies based on library names, library age etc.
- Policies based on licensing terms and licensing
- Policies based on vulnerabilities scoring, specific IDs etc.



Proprietary Vulnerabilities & Security **Database**

- Vulnerability Information from various sources including
- NVD, CNVD, CNNVD
- SCMs like Github, Gitlab, Bitbucket
- Public Commits on popular libraries
- Bug trackers like Bugzilla and Confluence
- 16 TB of data updated every 6 hours
- Popular and legacy open source libraries with high accuracy: 10 widely used languages and 15 binary formats
- Proactive checks for new vulnerabilities for your projects and automated alerts on outdated projects

Integrations to major SDLC products



- IDE Integrations for instant scan results for your developers
- Source Control Management Integration for ease of scanning detection of change in codes for each push or pull request
- Continuous Integration Tools to trigger automatic scans after builds are triggered for more comprehensive and accurate scan results on your projects
- Issue Management Tools to alert your developers of vulnerabilities being detected and assigning tickets for remediation within your team

Binary Analysis



• Scantist supports true binary analysis - going beyond strings and hashes and all things trivial to find open source risks in your applications

Docker Images Scanning



• Scantist supports detection of open source components from source-code, binary and environment dependencies.

•Prioritise remediation efforts using Scantist's security and compatibility assessment and relevant reference links

•Faster security fix time with recommended root-level fixes for developers that are easy to implement

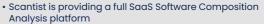
from verified sources

- Single-click fixes for all vulnerabilities
- •In-built issue management to enable clear delegation and tracking of issues (JIRA/Github and more)



Targeted & Actionable Remediation

SaaS / On-premise



• On-premise deployments and private cloud deployments are fully supported by Scantist SCA - contact us to find out more

INTEGRATIONS AND SUPPORT



SCM/Build Tools

• Bamboo • Bitbucket • Circle • Github • Gitlab • Jenkins • Travis

Languages	Package Managers	
Java	Maven	
	Gradle	
	Ant	
	Kotlin	
Javascript	NPM	
	Yam	
Python	pip	
C/C++	-	
Objective.C	CocoaPods	
CPAN	Perl	
Go	Go Modules	
Ruby	RubyGems	
PHP	Composer	
Swift	Swift	
Scala	Scala	

Binary File Formats	Supported Formats	
Bytecode	.jar, .war, .ear, .aar	
Binary Archive	.zip, .rar, .7z, .tar, .tar.gz	
Binary Files	.so, .o, .dll, .a, .lib, .elf, .exe, .com, .bin, .deb, .msi, .rpm, .ko, .sys, .dylib	
Mobile	.apk, .xapk, .aab	



OUR PLANS



Choose from our Basic, Premium

or Enterprise plans based on your development needs		Personal	Premium	Enterprise	
		Free	USD \$399 per developer per year	Speak with us	
		Unlimited number of projects and scans			
Scan Capacity	Number of Developers	1	Min 5	Min 20	
	Event or Time Triggered Scans	-	✓	✓	
	Admin service accounts	_	_	✓	
Binary Scans	Support binary scans	_	5МВ	>5MB	
Software Bill of Material	OSS Components per project	✓	✓	✓	
Vulnerability Info	Scan for CVEs	Limited	✓	✓	
	Priority Scoring of vulnerabilities	✓	✓	✓	
	Fix Recommendation Prioritisation	Limited	✓	✓	
	Scan for Security Warning & Bugs	-	✓	✓	
	Recommended Code Fix	-	Limited	✓	
Compliance Management and Rules	Compliance management	-	✓	✓	
	Policy Rules Customization	-	✓	✓	
Organization Management	Teams & Groups	-	✓	✓	
Reporting	Download Reports	✓	✓	✓	
	Knowledge Graph	-	✓	✓	
Integrations	Source code integrations (GitHub, GitLab, Bitbucket & Azure Repos)	Cloud only	Cloud only	Cloud and self hosted	
	CI/CD pipeline integration	✓	✓	✓	
	Jira, Slack & Rocket Chat integration	-	✓	✓	
	API Access	-	-	✓	
	Single Sign-on	_	_	✓	
Deployment	Deployment	Cloud	Cloud	Cloud or On-Site	
	New features in Beta version	-	-	Beta version available	
Support	Customer Support	Self help	Email support	Email and phone support	
	Account Manager	Self help	Shared	Dedicated	
	Costum SLA & Legal terms	_	_	✓	
	*Optional add-ons – Air-ad	an deployment and DevSec	One training		