

ReversingLabs Software Supply Chain Security

Features

Custom policy enforcement

- Determine what to scan for and how alerts are classified

In-depth threat hunting

Use the world's largest private repository of malware and goodware to find threats

Interactive reporting

- Automatically collect and save HTML reports with every scan to easily share and find specific components and vulnerabilities

Contextual alerting

- Receive alerts ranked by severity with recommended remediation steps

Secrets Leakage Prevention

- Reduce exposed secrets and sensitive information by prioritizing and suppressing alerts to reduce noise and improve response times

Software Bill of Materials

- Visualize your attack surface by seeing the open source and third-party software components in your environment

Digital signature validation

- Discover invalid, malformed, or altered signatures and certifications

Malicious behavior detection

- Discover abnormal behaviors and determine if they should be investigated

Vulnerability detection

- Find common vulnerabilities to manage common risks

Pre-production scanning

- Locate threats before updates or components are deployed or integrated

Security posture analysis

- Know your security maturity level and how to improve it

Third party risk management

- Understand if product updates are safe to deploy

Open Source Security

- Determine if Open Source components are safe to integrate into your environment

Summary

Security teams must adapt to new and expansive attack vectors and surfaces, commonly needing to go a step further than SCA tools to be protected from highly targeted, sophisticated supply chain attacks, rather than being protected from just vulnerabilities. ReversingLabs SSCS is a supply chain security platform that scans hundreds of file formats to identify embedded threats and integrates with CI/CD, cloud, and ITSM tools to automate testing, enforce policies, and establish security guardrails. It supports continuous, customized, and extensive coverage for third-party software and open source components.

Assess Your Risk

Continuously collect software bills of material (SBOMs) and risk reports, which follow the CycloneDX and SPDX format, and review each component's supplier, version, relationship with other dependencies, and embedded threats and vulnerabilities.

Find Your Threats

Review executables, components, and dependencies to monitor behaviors and detect suspicious changes in build systems, workflows, and large packages. Discover threats with scanning from the world's largest private repository of goodware and malware.

Consistently Remediate Threats

Automatically enforce risk-based policy controls, verify that severe issues are remediated, track your security posture, and support custom scanning where you can specify what to scan for, how alerts are prioritized, and review recommended steps for remediation with every alert.

SSCS Technical Specifications

File and software scanning	Malware scanning	Open API Integrations	Depth of coverage
Reviews 400+ file formats	15 billion total malware samples	Open Source Packages: ReversingLabs can analyze open source packages to ensure that their distribution from internal repositories do not contain malware	Languages: <ul style="list-style-type: none">• Java• .NET• Python• JavaScript• Shell scripts (e.g. Autot, Bash, PowerShell and Batch)• PHP• Delphi• Visual Basic• C/C++
Identifies open source, third-party and proprietary software, dependencies, installation, and container components	8 million samples are added daily	CI/CD: The CLI allows scanning to be integrated into any CI/CD tool and workflow, ensuring that builds are automatically reviewed for threats before they are released	
Identifies 4,800+ file types	46 different malware scanners		Platforms: <ul style="list-style-type: none">• Windows• Linux• Docker• Plug-ins for browsers & CI/CD toolchains
Scans software packages up to 10GB			
Identifies 250+ types of secrets such as credentials, passwords, API tokens, and encryption keys			Non-executable files, documents, multimedia and archives: <ul style="list-style-type: none">• MSOffice• Adobe PDF

Get Started!

We'll Show You How To Reduce Software Supply Chain Risks With ReversingLabs

www.reversinglabs.com

REQUEST A DEMO

About ReversingLabs

With cloud-native and on-prem support, ReversingLabs enforces custom policies, in-depth malware and tampering detection as well as contextual alerting across thousands of file types and many operating systems. Our solutions provide powerful scanning, fast remediation of supply chain threats, and the removal of coverage gaps from legacy application security tools.

Experience advanced software supply chain security today with a free trial of ReversingLabs SSCS and start finding the threats your other tools cannot find. SSCS uncovers operational risks while providing the coverage and information necessary to manage and remediate them.