Contrast SECURITY

# Contrast SCA: From Repo to Runtime – Full Spectrum Software Composition Analysis Across the SDLC

# Challenges

Open Source Software (OSS) affords developers many freedoms to build feature-rich applications on aggressive timelines. However, reliance on OSS adds layers of complexity across an organization's software supply chain. Some of the resulting risks are as follows:

### RISK FROM INACTIVE LIBRARIES AND CLASSES

The 2021 State of Open Source Security Report from Contrast Security found that 62% of libraries found in applications are inactive—that is, not used at all by the software in runtime.[1] And within active libraries, only 31% of library classes are invoked by the application. The derivative outtake is that only 9.4% of code in applications is active library and class code. As a result, developers are often overwhelmed by high volumes of erroneous security findings and do not have the means to prioritize their most utilized and at-risk libraries.

### DEPENDENCY RISK

Dependencies introduced during continuous integration/continuous deployment (CI/CD) workflows create additional layers of unaccounted risk. For example, new attack vectors like dependency confusion, in which attackers trick an application into using the wrong library, can be a vehicle for malicious code.[2]

### LEGAL AND COMPLIANCE RISK

Third-party software presents a variety of organizational risks that must be managed. For instance, some third- party libraries use risky licenses that could require an organization to open-source an entire application.[3] In response, application security teams need an automated means to baseline their SCA security posture while legal and compliance teams need to track licensing risk by building a software bill of materials (SBoM) that scales with their application portfolio.

# Solution

These and other risks make safeguards like software composition analysis (SCA) a necessity to ensure visibility and governance into the code developers are shipping. From repository to runtime, Contrast SCA provides organizations with full spectrum SCA across the entire software development lifecycle. By using a single platform for both static and runtime analysis and protection, organizations can simplify their security workflow and ensure their applications are secure from the start. Contrast SCA provides visibility into dependencies and known vulnerabilities in code repositories. Contrast SCA currently supports GitHub and plans to extend functionality to GitLab and Bitbucket, providing customers with even greater flexibility and choice when it comes to securing their applications.

Customers can shift smart with Contrast as they can get early feedback on security risk during development with the repository integration and accurate feedback during testing with agent technologies. Customers will no longer have to set up SCA one by one for each code repository.

Contrast SCA delivers real-time feedback into third- party software risk by embedding Software Composition Analysis and compliance controls into applications throughout their life cycle. By leveraging instrumentation, Contrast SCA reduces friction between development, security, and operations teams by showcasing critical insights, such as runtime library usage, that can help drastically reduce manual triaging and prioritize remediation efforts for developers.

Contrast SCA provides real-time feedback to developers by integrating into their native CI/CD workflows. It provides context into how vulnerable libraries are introduced—no scanning required. This enables developers to take advantage of the many benefits of SCA while providing application security teams the necessary safeguards they need to be confident that the libraries used in their code are secure.

### CAPABILITIES

- Prioritize remediation efforts by accurately identifying whether vulnerable open-source libraries are actually used by the application—all the way down to the specific class, file, or module.
- Flag dependency risk and contextualize how vulnerable dependencies are introduced and highlight potential supply chain attack vectors like dependency confusion.
- Check for vulnerable libraries before commit and institute security and license governance in native CI/CD workflows with the Contrast Command Line Interface (CLI).
- Automatically catalog third-party software assets—both commercial off-the-shelf (COTS) and OSS—and receive alerts when new vulnerabilities are detected in deployed libraries.
- Automatically create and maintain an organization-wide inventory of open-source components mapped to applications, servers, and environments to identify what runs where and what needs to be secured.
- Continuously evaluate OSS components in the application portfolio for both open-source vulnerabilities and open-source license risk.
- Set and automatically enforce custom OSS security and license policies within native CI/CD workflows and provide real-time feedback to security and development teams.

# Key Benefits

### ENABLE FASTER REMEDIATION BY PRIORITIZING THE VULNERABILITIES THAT MATTER

Because Contrast SCA can identify active library components down to the class, module, or file, this extra layer of insight allows security and development teams to prioritize remediation efforts by identifying the most heavily used libraries. This enables developers to avoid hours of remediating vulnerabilities in inactive code and verifying results.

### EMBED SECURITY WHILE ELIMINATING BOTTLENECKS WITH END-TO-END AUTOMATION

Contrast SCA inventories libraries and vulnerabilities within native CI/CD workflows with no manual scanning or false positives that distract developers from shipping code on time. Instead, Contrast SCA embeds into existing testing and build tools to provide real-time insights into third-party software assets. An embedded approach to SCA ensures dramatically fewer false positives—and results in less overwhelmed development and security teams.

## CONTINUOUS VISIBILITY INTO YOUR SOFTWARE SUPPLY CHAIN

Contrast SCA monitors the entire application portfolio, including third-party and custom code, automatically applying new vulnerability intelligence for libraries already deployed. This eliminates the need for disruptive scans and re-scans of code repositories. Beyond top-level library CVEs, Contrast SCA benchmarks dependency risk by highlighting vulnerable dependencies introduced during native-build processes and flags dependency confusion risk. For early security testing, the Contrast CLI enables developers to rapidly test to their code to check for vulnerable libraries and dependency risk before committing.

## SCALABLE GOVERNANCE WITHOUT IMPEDING INNOVATION

Contrast SCA automatically discovers open-source components in applications, provides critical versioning and usage information, and triggers alerts when risks and policy violations are detected at any stage of the software development life cycle (SDLC). Contrast SCA enables application security teams to institute custom policy standards across their entire application portfolio and to manage the use of open-source libraries and licenses within the software development workflow.

## SINGLE DEPLOYMENT TO RAPIDLY RESPOND TO NEW THREATS

The Contrast Secure Coding Platform leverages a single deployment and assessment process to identify vulnerabilities in open-source and custom code. There is no need to implement multiple tools, orchestrate between different analysis engines, or run complex correlations. Beyond automatically detecting risk, Contrast provides runtime protection so that attacks on vulnerable open-source code are automatically monitored and blocked to prevent exploitation in production.

[1] "2021 State of Software Composition Analysis Report," Contrast Security, April 8, 2021.
[2] Matt Austin, "Dependency Confusion: A New Third-party Risk for the Software Factory," Contrast Security, February 24, 2021.
[3] Thomas Claburn, "Ruby Off the Rails, Code Linrary Yanked over License Blunder, Sparks Chaos for Half a Million Projects," The Register, March 25, 2021.

**Contrast Security provides the industry's most modern and comprehensive Application Security Platform,** removing security roadblocks inefficiencies and empowering enterprises to write and release secure application code faster. Embedding code analysis and attack prevention directly into software with instrumentation, the Contrast platform automatically detects vulnerabilities while developers write code, eliminates false positives, and provides context-specific how-to-fix guidance for easy and fast vulnerability remediation. Doing so enables application and development teams to collaborate more effectively and to innovate faster while accelerating digital transformation initiatives. This is why a growing number of the world's largest private and public sector organizations rely on Contrast to secure their applications in development and extend protection in production.

**240 3rd Street**
**2nd Floor**
**Los Altos, CA 94022**
**Phone: 888.371.1333**