SOLUTION BRIEF

Contrast Software Composition Analysis (SCA)

Target actual threats, minimizing false positives from static SCA tools

Software development relies on open-source and third-party software and libraries to accelerate innovation and build feature-rich applications. These components can introduce significant challenges related to visibility, governance and security risks across an organization's software supply chain. Traditional Software Composition Analysis (SCA) solutions do not detect which libraries are called in runtime and the dependencies associated with them, so development and security teams clash over what constitutes exploitable code.

Contrast SCA helps teams focus on the risks that matter by analyzing which libraries are used during the application runtime, right down to the specific class, file or module. It automatically creates an inventory of an organization's software and libraries while providing continuous observability into new vulnerabilities, with no manual scanning required.

Risks from third-party software and libraries require runtime application security

Organizations struggle to maintain an accurate inventory of all open-source and third-party components used in their applications, making it difficult to track vulnerabilities and ensure compliance.

Only 54% of major code changes undergo a full security review before deployment to production, meaning almost half of major application code changes are not thoroughly vetted.[1]

Attackers exploit new vulnerabilities in as little as five days, yet it takes development teams an average of 84 days to patch the most critical flaws. This troubling gap is widened by the sheer volume of new threats, with applications facing 17 new vulnerabilities monthly while developer teams on average are remediating 6 per month.[2]

Managing third-party software risks require the quickest possible turnaround for resolving issues once they emerge. Open-source vulnerabilities that can be exploited are valuable on the dark market. For example, information about undocumented vulnerabilities in popular software that can give root or equivalent access sells for as much as $1 million.[3]

But even when these zero-day vulnerabilities are eventually discovered and disclosed, it can take teams months to apply all patches and push them to production.[4]

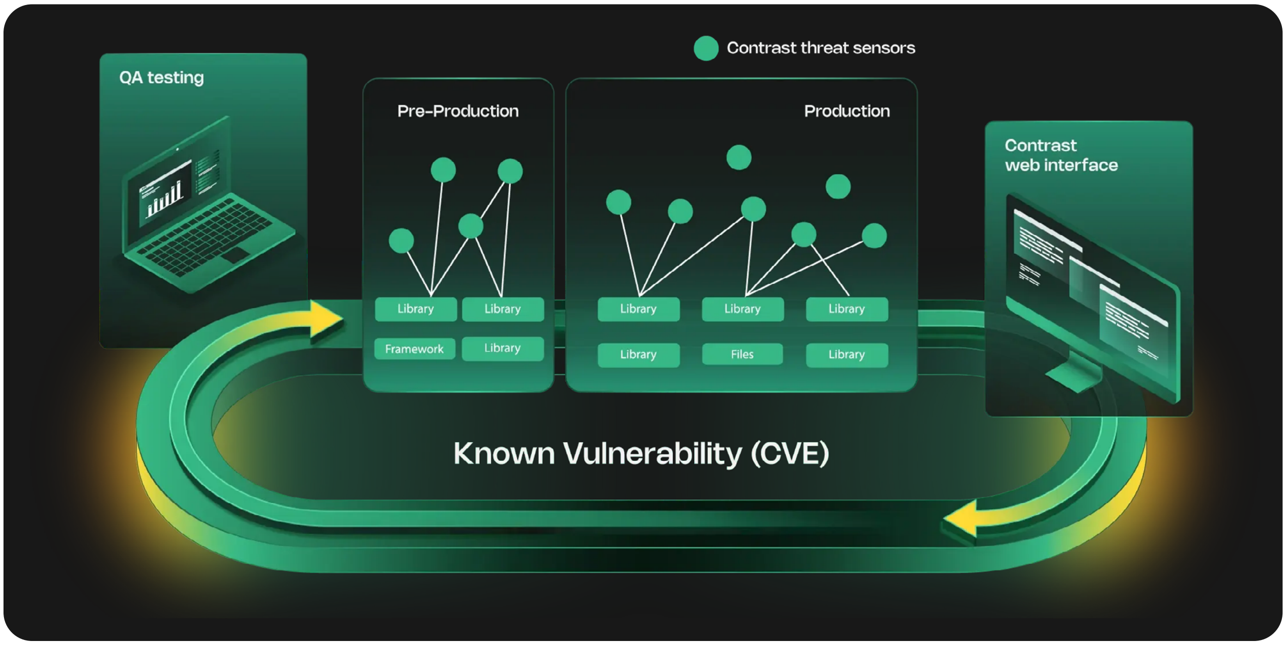
Traditional SCA tools often flag every known vulnerability in a library, regardless of whether the vulnerable code is actively used by the application. This leads to a flood of false positives, causing alert fatigue and diverting developer attention from real threats. Studies show that 62% of libraries within applications are inactive, meaning they are not used at all by the software during runtime.[5]

Additionally, most of today's security testing solutions offer limited guidance for fixing vulnerabilities, which directly contributes to a growing backlog of unfixed vulnerabilities. If information about a vulnerability is provided at all, it lacks "how-to-fix" instructions geared for non-experts to help developers to quickly fix code issues.

To simplify the management of third-party and open-source software and libraries components and reduce application vulnerabilities across the Software Development Life Cycle (SDLC), teams need full awareness of their software risks.

A concerted effort to remediate the vulnerabilities that put businesses at risk and "pay down" their security debt is the single most powerful action a company can take to reduce the chance of a breach.[6]

Full SCA testing coverage across the entire software development lifecycle



Deep application instrumentation to provide unparalleled accuracy and context

Contrast SCA offers a unique, embedded approach to Software Composition Analysis (SCA) that removes much of the overhead from application security and development teams. Unlike traditional SCA tools that only provide point-in-time assessments, Contrast SCA embeds sensors within the application to continuously evaluate third-party libraries at runtime. This eliminates the need for a separate assessment with different tools. There are no scans to manage and no extra steps for developers — just continuous insight. Contrast SCA detects which open-source libraries are called in runtime, the dependencies associated with them, and if they are exposing the organization to unnecessary security risks or legal problems due to open-source licensing complications.

Runtime-aware analysis

Uniquely analyzes which open-source and third-party libraries are used by the application during runtime, down to the specific class, file or module. This eliminates noise by focusing only on exploitable vulnerabilities in active code, drastically reducing false positives.

Automated inventory and SBOM

Automatically creates a comprehensive Software Bill of Materials (SBOM) for all open-source and commercial libraries, providing a clear inventory and continuous observability into new vulnerabilities without the need for manual scanning.

Prioritized remediation

Prioritizes vulnerabilities by understanding active usage, based on true risk and exploitability, guiding developers to fix the most critical issues first.

Highlight transitive dependencies

Run quick tests for vulnerable top-level libraries prior to committing code to highlight transitive dependencies introduced during the build process by populating a dependency tree within Contrast SCA.

Learn more

[1] CrowdStrike 2024 State of Application Secuirty Report
[2] Software Under Siege 2025 Report
[3] How To Start Decluttering Application Security
[4] Why Lack of Application Security Skills and Experts Hamstrings Digital Transformation Initiatives
[5] The State of Open Source Security
[6] How To Get Out Of Security Debt

Contrast Security is the world's leader in Runtime Application Security, embedding code analysis and attack prevention directly into software. Contrast's patented security instrumentation enables powerful Application Security Testing and Application Detection and Response, allowing developers, AppSec teams and SecOps teams to better protect and defend their applications against the ever-evolving threat landscape.

contrastsecurity.com

6800 Koll Center Parkway
Ste 235
Pleasanton, CA 94566
Phone: 888.371.1333