Contrast Scan:
Pipeline-Native Static Application Security Testing

Contrast Scan's pipeline-native static analysis engine is built to run in modern CI/CD pipelines with industry-leading speed and accuracy, making security testing as routine as committing code.

Challenges with SAST Today

Static application security testing (SAST), is a cornerstone in many enterprise DevSecOps programs. However, for the past 20 years, businesses have relied on clunky, antiquated SAST tools that produce thousands of false positives and take hours (or days) to scan, which can only be helped by manually configuring security rules. Conversely, niche developer tools that plug into the IDE or source code repository miss the mark on finding real, exploitable vulnerabilities, leaving major security gaps across your application layer.

Contrast Scan is Made for Modern Development Pipelines

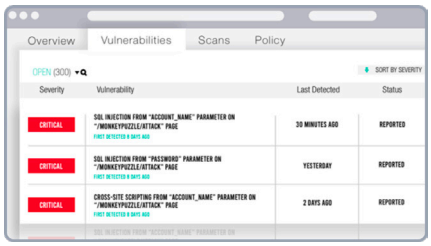
Contrast Scan is a SAST solution purpose-built to run in modern development pipelines. By integrating into developer CI/CD tooling, Contrast makes security testing as routine as a commit or pull request. With actionable remediation guidance pointing to the specific line of code, developers can secure as they code without ever leaving their environment.

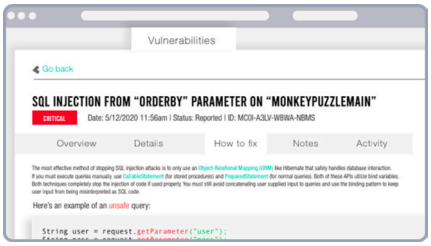
Contrast Scan is among the fastest and most accurate SAST tools on the market. Period. Using a risk-based scanning algorithm and security ruleset, Contrast Scan zeroes in on vulnerabilities that pose real risk by performing deep analysis on exploitable data paths while filtering out noise from false positives by up to 80%. Because Contrast Scan prioritizes real risk, developers and security teams can expect scan times up to 15x faster than legacy SAST tools.

How Contrast Scan Delivers

Pipeline-Native Integrations
Contrast Scan is built from the ground up to run within any modern pipeline as opposed to operating as a cumbersome gate prior to release. This ensures security is embedded as a routine step of the CI/CD pipeline and gives developers the freedom they need to secure as they code. Scans can be run on commit or pull request, through a simple-to-use command-line (CLI) option, build automation, API call or a secure code upload through the Contrast UI.

Risk Based Scanning Engine
A breakthrough code scanning algorithm powers the static analysis engine in Contrast Scan, enabling teams to pinpoint exploitable vulnerabilities while ignoring those that pose no risk and only cause hours of needless triage. Because the engine powering Contrast Scan focuses on exploitable flaws only, based on real-world scan results, Contrast Scan can shrink the amount of time to run scans by up to 15x, with accuracy scores up to 80% higher than legacy SAST tools.





Actionable Remediation Guidance
Contrast Scan provides "how-to-fix" guidance down to the specific line of code, providing instant feedback to developers within CI builds and PRs. Developers don't need advanced security expertise or training to make fixes to their code directly within their pipeline environment.

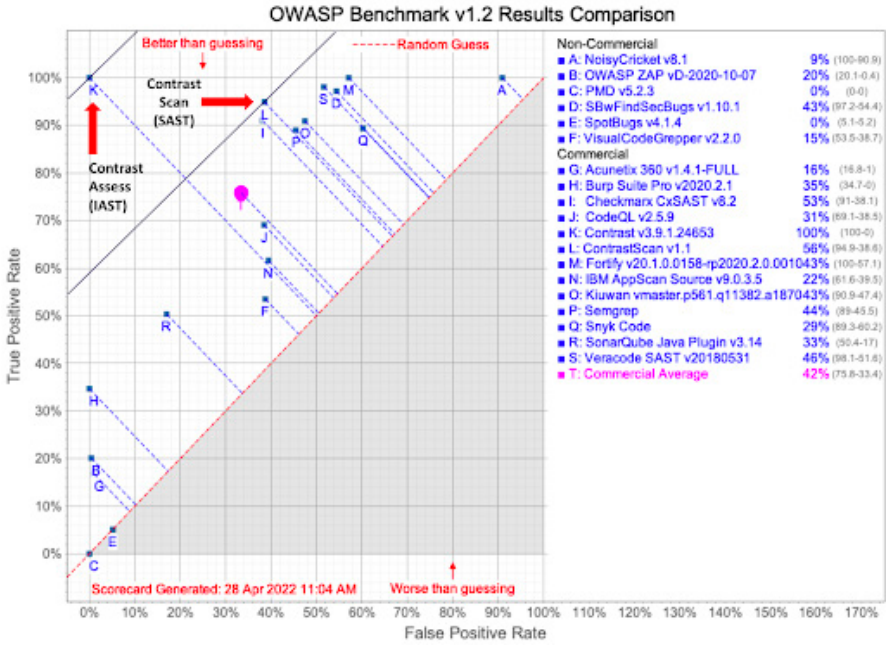
How Contrast Stacks Up to the Competition

The World's Fastest Scanner
Contrast Scan produces results with scan times that can be measured in seconds, not hours. Testing on a 84Mb Java application yielded results in just over 1 minute, up to 15x faster than competing commercial SAST tools which took nearly 17 minutes to scan the same application.

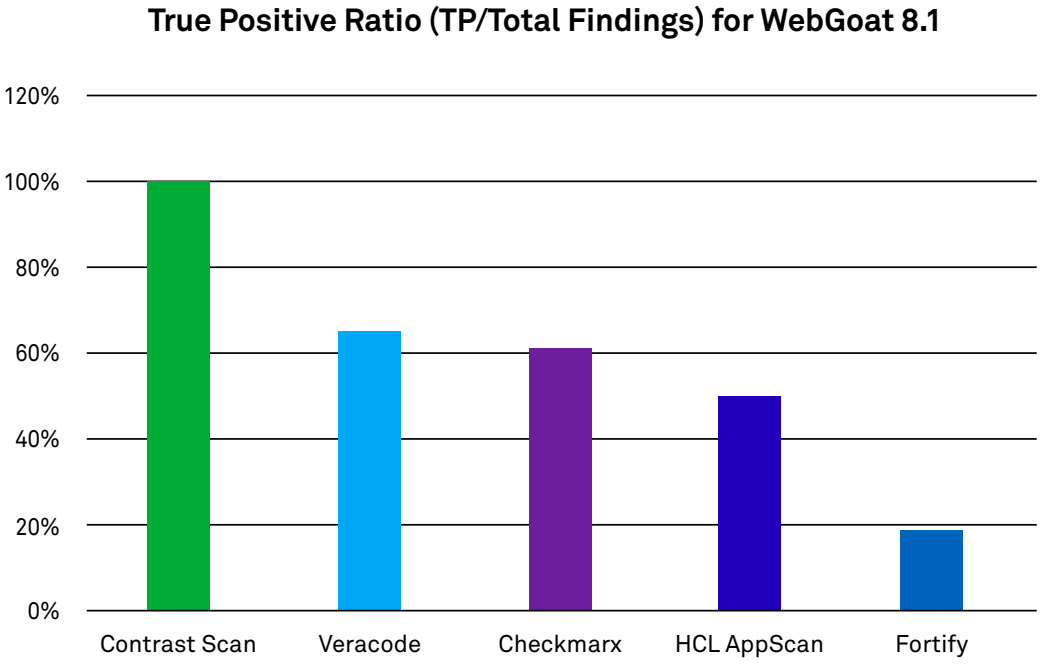
Scan Times for WebGoat 8.1 in Minutes (App Size: 84Mb)	
Contrast Scan	**1:06**
HCL AppScan	2:59
Veracode	14:00
Checkmarx	14:00
Micro Focus Fortify	16:56

Laser Focused Findings Without the Noise

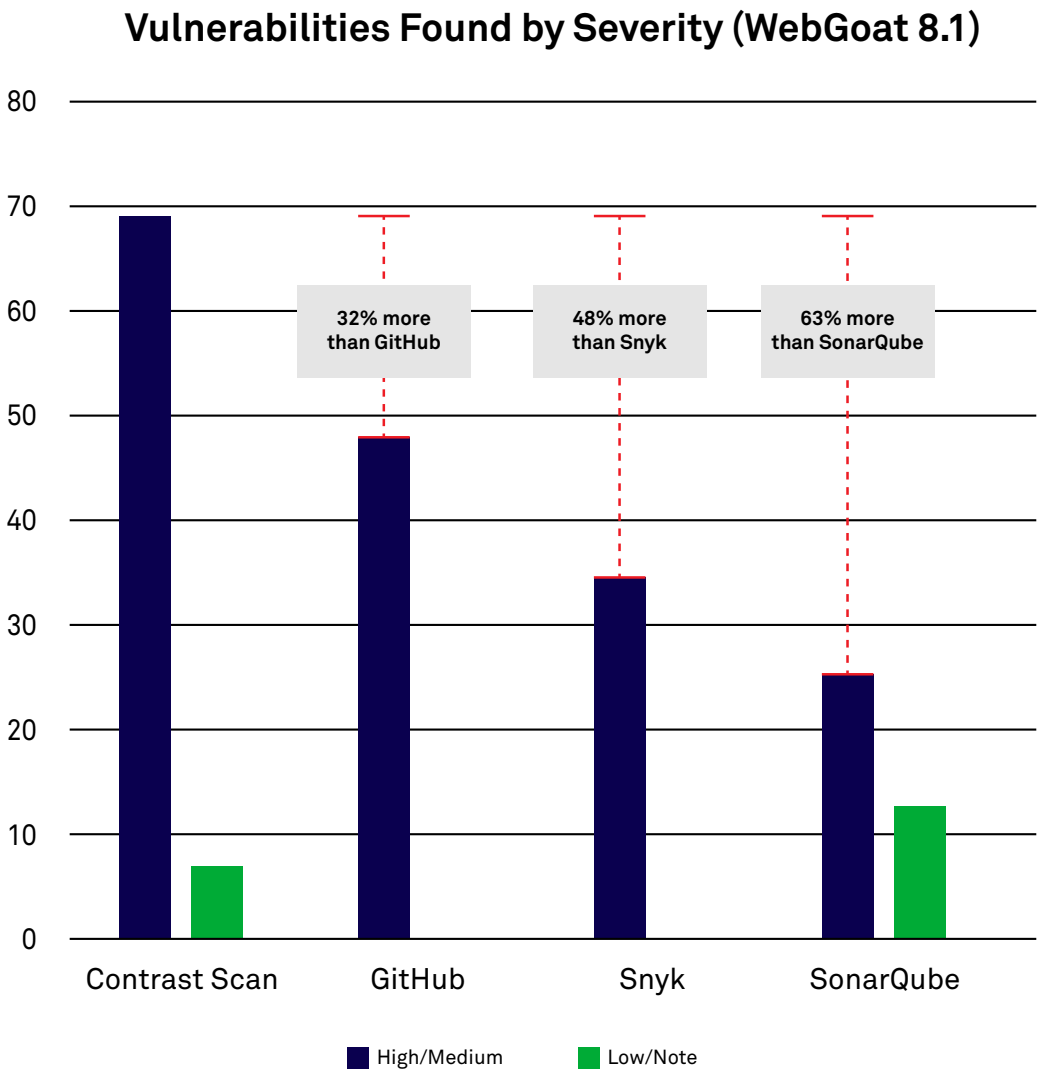
Contrast's SAST engine uses a risk-focused algorithm and security rules that prioritize exploitable findings. Contrast Scan performs deep analysis on exploitable data paths and categorizes security findings based on which ones require immediate attention while ignoring erroneous false positives that only create hours of needless triage.



Contrast Leads the Pack in the OWASP Benchmark



Contrast Scan Produces the Least Amount of Noise Among Commercial SAST Tools



Contrast Finds an Average of 48% More Vulnerabilities Than "Developer Friendly" Tools

Laser Focused Findings Without the Noise

Contrast CodeSec, Contrast's free-to-use developer security tool, utilizes the same pipeline-native SAST engine as the enterprise version of Contrast Scan delivered through an easy-to-use CLI command. Developers can take advantage of industry-leading speed, accuracy and actionable how-to-fix guidance on their local machine without ever leaving their pipeline.

Try for free today at **contrastsecurity.com/developer**.