SOLUTION BRIEF

# Contrast Code

## Bridge the gap from code to production

*Unify static repository data with real-time execution context to find, prioritize and fix what actually matters.*

### The problem: AppSec noise and remediation fatigue

AppSec teams struggle to show progress because they rely on data from traditional application security tools, which lack the context needed to separate real threats from noise, leaving them buried under a mountain of unprioritized alerts.

- **82% false-positive rates:**[1] Traditional scanners produce excessive noise, burying real risks.
- **270 days to remediate:**[2] The average time to fix a vulnerability is nearly nine months.
- **30% of alerts uninvestigated:**[3] Security teams are forced to ignore nearly a third of alerts due to lack of bandwidth.

The rise of AI agent-based coding has pushed development speed to unprecedented levels, but it also exposes the limits of analysis without runtime context. When scanning operates in a silo, the massive volume of code exponentially multiplies the noise.

Organizations are forced into a lose-lose scenario: slow down development pipelines over theoretical vulnerabilities, destroying the speed gains of AI workflows, or bypass controls entirely and push vulnerable code directly to production. To secure an autonomous pipeline, organizations need automated security gates that only trigger on proven, exploitable risk.

### Why runtime context matters for AppSec

Organizations today are managing application security across fragmented tool sets, each generating its own findings in isolation. Without a way to correlate what scanners find in code with how applications actually behave in production, AppSec teams can't answer the most basic question: Which of these vulnerabilities are actually exploitable?

The absence of runtime context makes it impossible to distinguish a critical threat from harmless background noise. Consequently, teams remain exposed to hidden risks while their resources are drained by the work of investigating irrelevant or unprioritized security alerts.

### The Contrast Code solution

Contrast Code is an AI-powered orchestration engine that integrates SAST and SCA findings with the Contrast platform to provide a complete runtime-aware view of application risk. With this approach, AppSec teams move beyond overwhelming noise and slow remediation to AI enrichment and triage validated against runtime results to prioritize top risks.

## How it works: Enhancing SAST and SCA with AI

### AI-powered triage

Contrast Code uses AI to analyze ingested SAST and SCA results. The platform then identifies likely false positives, removes duplicates and triages the data. This reduces the volume of findings that require input from your team.

### Vulnerability accuracy

Those static findings are then correlated with runtime observations from the Contrast Platform, so teams can see which vulnerabilities exist in code that is actually exercised in production. The result is a shorter, higher-confidence list of issues worth acting on.

### Automatic prioritization

Contrast Code assigns a Contrast Score based on source severity, CVSS data and runtime correlation. This score drives prioritization, ensuring that exploitable, production-relevant risks surface first. AppSec teams spend less time manually sorting through findings and more time driving remediation where it has real impact.

### Key benefits

- **Unified view with broad language coverage:** AppSec and developers have a comprehensive view of vulnerabilities across major languages from dev to prod.
- **AI enrichment:** AI-powered triage analyzes findings, flags false positives and provides reasoning to save developers time.
- **Runtime correlation:** Correlate SAST with runtime data, identify which vulnerabilities are actually reachable and exploitable, and prioritize real risks over theoretical ones.

With Contrast Code, teams gain broader coverage and sharper prioritization through the Contrast runtime security platform. This unified platform equips developers, AppSec and SecOps teams to proactively protect and defend applications and APIs against evolving threats without slowing teams down. With the Contrast runtime security platform, teams have a continuous feedback loop that connects vulnerabilities found during development with threats detected in production.

Request a demo

[1] The Truth About AppSec False Positives
[2] 2025 State of Vulnerability Management & Remediation Report
[3] The Cybersecurity Alert Fatigue Epidemic

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