SOLUTION BRIEF

Contrast Scan

Static code scanning tool with remediation guidance

Traditional static application security scanning tools were not designed to be built into a development pipeline, nor to support the spread of today's distributed applications. They are slow, generate noisy results, and require analysts to parse findings before remediation can begin. As a result, these legacy testing tools often force organizations to choose between speed and security.

Contrast Scan delivers speed by integrating application vulnerability detection into the development pipeline. It helps organizations simplify operations, significantly accelerate vulnerability remediation processes and deliver secure code.

DevOps requires an updated approach to software scan testing

Traditional Static Application Security Testing (SAST) scanning solutions attempt to build a model of an application in order to project the application's runtime behavior and subsequently the vulnerabilities in it. This approach produces high volumes of false positives that must be painstakingly triaged and diagnosed before they can be passed to developers to remediate. When it comes to accuracy, traditional SAST solutions might flag a piece of code that looks like it could be risky, but it can't tell if an attacker can actually control the information going into that code, or if you already have other security measures in place to prevent problems.

Traditional scanning tools are slow, compute intensive, and expensive. Lengthy scan times can impede or even stall development pipelines and prolong delivery cycles. These antiquated approaches were not built for today's Continuous Integration/Continuous Deployment (CI/CD) pipelines and therefore require anywhere from one hour to 7+ days per scan.[1] Most organizations (91%) report that their vulnerability scans take at least three hours.[2]

The vast majority of organizations (73%) report that each security alert they receive consumes an hour or more of application security time.[3] Further, 72% of organizations indicate that true vulnerabilities consume 6+ hours of application security team time; 68% say that true vulnerabilities consume 10+ hours of development team time.[4] Fixing a vulnerability gets more expensive as the development process gets further from where the error was introduced.[5]

Additionally, most of today's security testing solutions offer limited guidance for fixing vulnerabilities — which directly contributes to agrowing backlog of unremediated 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.

Poor "how-to-fix" guidance has a measurable impact for the average organization because it can take up to 121 days to fix only 50% of issues.[6] Plus, businesses that carry more security debt can experience a 1.7x higher volume of vulnerabilities.[7]

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.[8]

To address all of these critical shortcomings that impact both application security and operational efficiency, organizations need a code-scanning tool that observes data flows and identifies application and API vulnerabilities that allow malicious attacks.

The entire SoftwareDevelopment Life Cycle (SDLC) empowers teams to run scans up to 10x faster and remediate vulnerabilities up to 45x faster while meeting compliance requirements of an organization's security policy. Unlike legacy scanning tools, Contrast's approach is designed specifically for integration with modern CI/CD environments, tooling and workflows.

Identify and fix code vulnerabilities faster with actionable data

Contrast Scan uses a risk-based analysis engine that helps to pinpoint exploitable vulnerabilities and produces results with scan times measured in seconds, not hours, zeroing in on vulnerabilities that pose real risk. It provides code-level, "how-to-fix" guidance for over 30 languages and frameworks. Security rules prioritize exploitable findings and ignore false positives.

Integrate with developer tools, repositories and build pipelines

Onboarding with Contrast Scan requires zero configuration and three clicks in a single CLI command to start scanning. In addition, simple, purpose-built tool plug-ins (e.g., Maven, Gradle, GitHub Actions) for CI/CD allow you to automate scans out of the box. Contrast Scan is integrated as part of the Contrast runtime security platform so organizations have a unified, developer-friendly view of vulnerabilities and attacks across SAST, Interactive Application Security Testing (IAST), runtime protection and observability and Software Composition Analysis (SCA).

Analysis on exploitable data paths

Contrast Scan's risk-based rule set focuses only on vulnerabilities that are actually exploitable. A demand-driven algorithm powers Contrast Scan's static analysis engine. This helps teams pinpoint and prioritize vulnerabilities that matter while ignoring those that pose no risk. As a result, Contrast's real-world scan results can shrink scan times by a factor of 10. Faster scans remove DevOps security roadblocks that slow innovation, improve the efficiencies of security and development teams, and subsequently help reduce operating expenses associated with scanning workflows. Contrast Scan also offers a Command-Line Interface (CLI) and extensible Application Programming Interfaces (APIs) for SDLC integrations.

Vulnerabilities fixed up to 45x faster, runtime protection for those that remain

Contrast Scan can accelerate remediation times up to 45x. This is achieved by enabling developers to focus on exploitable flows, prioritize routes with entry points based on runtime and production traffic analysis, and leverage actionable, context-rich, "how-to-fix" guidance. All of this pays down security debt, which results in reduced application security risks.

Accellerate delivery cycles: 30% improvement in application security efficiencies

Application security teams can improve their scan, triage, and remediation efficiencies by nearly a third (up to 30%). Contrast's comprehensive DevSecOps approach bakes security into rapid-release cycles that are typical of modern application development and deployment environments. It also offers complete coverage of the DevSecOps life cycle, providing optimized tools from build to production. Contrast can also help streamline compliance reporting by shrinking the time needed for policy auditing and reporting workflows from days to minutes.

One platform: Scan for build, assess for test, protect for run

The Contrast runtime security platform was purpose-built to deliver harmonized analysis, testing, and exploit prevention capabilities via instrumentation across the entire life span of an application. Contrast Scan enhances modern security capabilities across each critical phase of the CI/CD pipeline:

Development

Contrast empowers developers to write secure software quickly by helping teams accurately identify and remediate vulnerabilities based on code scans.

Test

Contrast runtime analysis helps validate, fix and assure secure software development.

Production

Contrast also helps software run securely by stopping attacks in production — both known and unknown application exploits.

The Contrast runtime security platform secures software across all stages of the SDLC. Its comprehensive suite of capabilities offers embedded, continuous testing and protection that reduce application security risks.

Contrast Scan's pipeline-native static analysis perfectly complements the Contrast platform with specific precision and performance advantages:

Built for development pipelines

With zero configuration setup, teams can start scans in three clicks.

Designed for faster scans

Offers best-in-class scan times.

Produces results that matter

Focuses on only the vulnerabilities that matter, generating results that are dramatically less noisy (80% fewer false positives).

Learn more

[1] Micro Focus Fortify Static Code Analyzer, Software Version: 18.10
[2,3] The State of DevSecOps Report
[4] 2021 State of Application Security in Financial Services Report
[5] How To Start Decluttering Application Security
[6] Why Lack of Application Security Skills and Experts Hamstrings Digital Transformation Initiatives
[7] Application Risk is 1.7x Higher for Organizations That Fail to Manage Security Debt
[8] 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