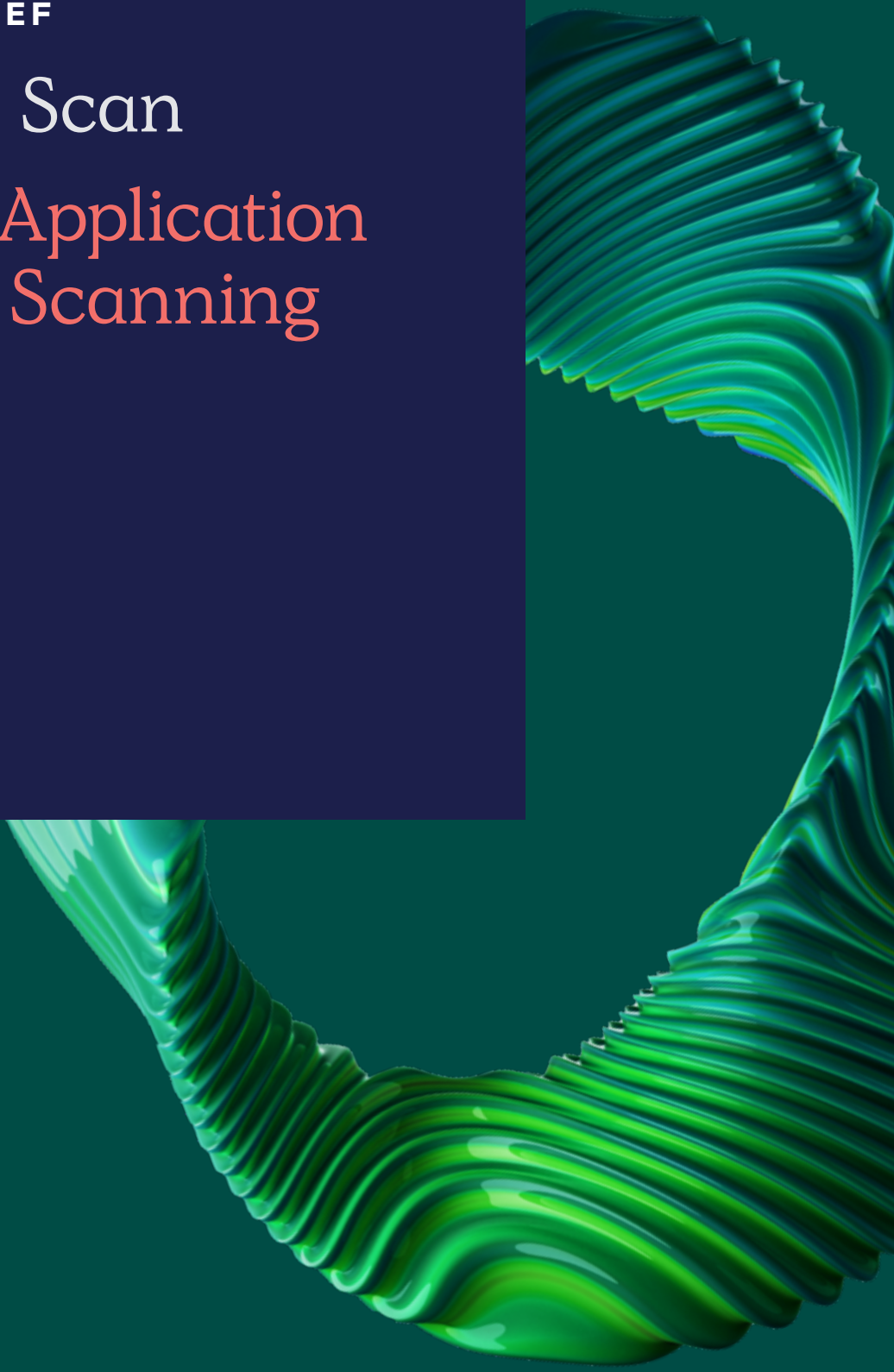
Contrast SECURITY

SOLUTION BRIEF

Contrast Scan

Modern Application Security Scanning



Executive summary

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 human security analysts to parse findings before remediation can begin. As a result, these legacy testing tools often force organizations to choose between speed and security.

As the latest addition to the Contrast Application Security Platform, Contrast Scan provides a pipeline-native static analysis solution that delivers speed, accuracy, and integration with modern development systems. It helps organizations simplify operations, significantly accelerate vulnerability remediation processes, and deliver secure code on aggressive schedules

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 a lot of alert noise—mixing high volumes of false positives with true vulnerabilities that must be painstakingly triaged and diagnosed before they can be passed to developers to remediate. When it comes to accuracy, traditional SAST solutions achieve a mere 26%.[1]

All of this alert noise tallies up to a huge time expenditure. The vast majority of organizations (73%) report that each security alert they receive consumes an hour or more of application security time.[2] 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.[3]

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 is typically not written with the developer in mind—lacking "how-to-fix" instructions geared for non-experts to help developers to quickly fix code issues.

> *Fixing a vulnerability gets more expensive as the development process gets further from where the error was introduced.*[4]

Contrast SECURITY

Poor "how-to-fix" guidance has a measurable impact—for the average organization it takes 121 days to fix only 50% of issues.[5] Plus, businesses that carry more security debt tend to fall further behind and experience higher volumes of vulnerabilities—1.7x higher than for organizations with below-average security debt.[6]

Finally, 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 hours or days to run—anywhere from one hour to 7+ days per scan.[8] Most organizations (91%) report that their vulnerability scans take at least three hours—and for 35%, they take eight or more hours.[9] The more traditional scans that an organization runs, the higher the cost to the company—and most SAST tools are recommended to be run on a daily basis.

To address all of these critical shortcomings that impact both application security and operational efficiency, organizations need a modern, pipeline-native static analysis solution. Contrast Scan extends the capabilities of the Contrast Application Security Platform to cover the entire software development life cycle (SDLC)—empowering teams to run scans up to 10x faster and remediate vulnerabilities up to 45x faster10 while meeting compliance requirements of an organization's security policy. And unlike legacy scanning tools, Contrast's approach is designed specifically for integration with modern CI/CD environments, tooling, and workflows.

> *A concerted effort to remediate the vulnerabilities that put businesses at risk and "pay down" their security debt (viz., an increasing number of unremediated vulnerabilities) is the single most powerful action a company can take to reduce the chance of a breach.*[7]

Contrast Scan: a revolutionary solution for pipeline-native static analysis

Contrast Scan realizes a pipeline-native approach to static analysis—one that achieves dramatic improvements in speed, accuracy, and developer experience by removing inefficiencies and roadblocks that slow release cycles. It delivers the fastest, most accurate staticanalysis scanner available today.

The combination of Contrast Scan with the other solutions in the Contrast Application Security Platform (Contrast Assess, Contrast SCA, and Contrast Protect) extends Contrast's true DevSecOps capabilities across the entire SLDC. And this makes shipping code with zero critical vulnerabilities a reality.

Contrast SECURITY

GET A WIN WITH DEVELOPERS: UP AND RUNNING IN THREE CLICKS, IN THE WAY DEVELOPERS KNOW AND LOVE

Onboarding with Contrast Scan is quick and easy—requiring zero configuration and literally 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. Further, as Contrast Scan is integrated as part of the Contrast Application Security Platform, 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).

SHIP SECURE CODE ON TIME: RESULTS THAT MATTER, DELIVERED 10X FASTER

Contrast Scan's smart, risk-based rule set focuses only on vulnerabilities that are actually exploitable. A breakthrough, 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 (OpEx) associated with scanning workflows. Contrast Scan also offers a command-line interface (CLI) and extensible application programming interfaces (APIs) for SDLC integrations.

ACTUALLY REDUCE RISK: VULNERABILITIES FIXED UP TO 45X FASTER, RUNTIME PROTECTION FOR THOSE THAT REMAIN

When used in concert with the broader set of capabilities in the Contrast platform, 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. The Contrast platform further supplements these capabilities by providing runtime protection for any open or unknown vulnerabilities in production.

ACCELERATE DELIVERY CYCLES: 30% IMPROVEMENT IN APPLICATION SECURITY EFFICIENCIES

By integrating pipeline-native static analysis security testing into the Contrast platform, 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— shrinking the time needed for policy auditing and reporting workflows from days to minutes.

Contrast SECURITY

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

The Contrast Application Security platform was purpose-built to deliver true DevSecOps with harmonized analysis, testing, and exploit prevention capabilities via instrumentation across the entire life span of an application. The addition of Contrast Scan to the Contrast platform 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 platform secures software across all stages of the SDLC. Its comprehensive suite of capabilities was built for modern, distributed applications—offering 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 from the ground up 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).

Contrast SECURITY

[1] "OWASP Benchmark v1.1, 1.2," OWASP, accessed April 19, 2021.
[2] "The State of DevSecOps Report," Contrast Security, December 2020.
[3] "2021 State of Application Security in Financial Services Report," Contrast Security, May 2021.
[4] Jeff Williams, "How To Start Decluttering Application Security," Forbes, January 27, 2021.
[5] "Why Lack of Application Security Skills and Experts Hamstrings Digital Transformation Initiatives," Contrast Security, July 13, 2020.
[6] Katharine Watson, "Application Risk Is 1.7x Higher for Organizations That Fail To Manage Security Debt," Contrast Security, July 24, 2020.
[7] Yaniv Bar-Yadan, "How To Get Out Of Security Debt," Forbes, September 3, 2020.
[8] "Micro Focus Fortify Static Code Analyzer, Software Version: 18.10," Micro Focus, May 2018.
[9] "The State of DevSecOps Report," Contrast Security, December 2020.
[10] 45x faster vulnerability remediation is based on measurement of the same guidance feature in the Contrast Assess IAST testing solution.

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
Fax: 650.397.4133

Contrast SECURITY

contrastsecurity.com