Contrast SECURITY

SOLUTION BRIEF

Automatically Identify Software Vulnerabilities and Verify their Remediation with Route Intelligence™

Executive Overview

Existing application security (AppSec) testing solutions are unable to provide security and development teams with comprehensive visibility across the entire application attack surface. At the same time, they squander limited staff resources on manual workflows associated with the identification and remediation of vulnerabilities.

The addition of Route Intelligence™ capabilities to Contrast Assess provides comprehensive visibility across all application routes while automating the workflows associated with vulnerability identification and remediation verification. This enables development teams to improve efficiencies, as well as speed code releases. At the same time, security teams have full visibility into applications—from development to production—and are able to recapture valuable time spent verifying vulnerability fixes.

Lack of Visibility Inhibits DevOps

Traditional approaches to AppSec testing have significant limitations. When development teams employ static application security testing (SAST) and dynamic application security testing (DAST) tools, they discover that they are inherently slow and their approach to checking every line of code is often redundant. Some of the challenges they face include:

- Static code analyzers only see a small portion of source code. They're unaware of which libraries have custom rules coverage. This results in false negatives.
- Dynamic scanners attack application programming interfaces (APIs) but are unaware of wildcard URL mappings. As a result, they overtest certain paths and undertest or ignore others. This results in false negatives that ratchet up risk.
- Manual penetration tests attempt to compensate for both of these issues. But the time frames for doing so are limited, and they may be unfamiliar with how application routes operate in various frameworks during runtime. This results in uncertainty of an individual application's actual vulnerabilities when it is in operation.

False Positives Create Inefficiencies and Risk

In addition, traditional AppSec methods cannot spot critical vulnerabilities due to the sheer volume of noise they encounter; false positives create confusion and frustrate both development and security teams. They are often overwhelmed and unsure as to which problem to tackle first. Specifically, while static testing methods may check every line of application code, these processes are both slow and ineffective because of a high volume of false positives. Further, static approaches are unable to trace data flows through bulk data structures—such as arrays, lists, and collections. These issues create noise that inhibits discovery of actual problems that cause risks when the code is running.

Contrast SECURITY

Identification that Misses Critical Vulnerabilities

Traditional SAST and DAST testing tools are incredibly slow because they build and scan hypothetical models of source code repositories. Their lack of discovery and comprehensive visibility capabilities yields an incomplete view of both the attack surface and vulnerability models. This is the reason that their test findings are peppered with false positives and cannot provide meaningful insight into risk prioritization.

As a result, vulnerability verification requires manual workflows. These are not only ineffective in spotting risks but they also eat up hundreds or thousands of valuable staff hours while slowing down continuous integration/continuous deployment (CI/CD) life cycles. Staff must sort through scores of false positives rather than writing code.

Web application vulnerabilities are by far the most common source for hacking-based breaches.[1]

How Does Traditional AppSec Address Vulnerabilities?

IDENTIFICATION OF VULNERABILITIES

Manual workflows where every line of code is taken out of development and tested for vulnerabilities.

VERIFICATION OF VULNERABILITIES REMEDIATED

Manual verification of vulnerability fixes conducted by developers and/or security staff.

ATTACK SURFACE VERIFIED

Every line of code inspected out of the development band.

Contrast Assess with Route Intelligence is the only AppSec testing solution that provides comprehensive attack surface visibility and automated verification.

Contrast SECURITY

Contrast Assess with Route Intelligence automates vulnerability identification and remediation verification by testing running applications. It also provides visibility into every application route instead of analyzing individual lines of code—which is the approach taken by traditional AppSec models.

Route Intelligence Reduces Application Risk

As part of Contrast's agent instrumentation-based AppSec platform, Contrast Assess runs in preproduction by gathering data from both custom code and open source libraries during normal running use—automatically enumerating remotely accessible parts of the application from the inside. Examples of routes include representational state transfer (REST) and Google remote procedure call (gRPC) endpoints.

Route Intelligence maps URLs to code paths to inform security testers of how the application is accessed, as well as if they have actually tested each route. Route Intelligence also maps vulnerabilities to routes, enabling teams to understand the level of authorization per route and accessibility of any discovered vulnerabilities.

These unique capabilities allow Contrast Assess to eliminate noise of false positives; this enables development teams to increase efficiencies while focusing on code releases. By identifying and analyzing every application route, Route Intelligence enables developers to also eliminate false negatives. The addition of Route Intelligence to Contrast Assess enhances AppSec testing capabilities in three ways:

UNWAVERING CONFIDENCE

The best way to understand how a modern application works doesn't come from looking at its lines of code, but rather at how users interact with an application when it is running. That real-time user interaction can be tested by observing the routes the application takes—and many URLs can map to a single route to introduce runtime vulnerabilities. Unlike traditional AppSec testing that builds and scans hypothetical models of source code repositories, Contrast Assess uses a patented instrumentation-based approach to directly interrogate application frameworks to determine all possible application routes to construct **full visibility of the entire application attack surface**.

BETTER VISIBILITY

Because of the discovery approach employed by Contrast Assess, developers have a full and complete picture of their entire application attack surface, how much of it has been tested, and what areas require remediation based on identified vulnerabilities. This dramatically **reduces the noise of false positives** during vulnerability testing, while helping developers prioritize which parts of the application to remediate first.

Contrast SECURITY

ADDITIONAL AUTOMATION

By utilizing an application's runtime behavior, Route Intelligence enables users of Contrast Assess to compare successive security assessment results for each application route to ensure that the vulnerability originally discovered on an entry point is no longer present. This **automated vulnerability remediation verification** approach dramatically improves application risk posture while giving back hundreds of hours annually to development teams. And this active methodology seamlessly fits into existing CI/CD pipelines—accelerating the process from development to production.

Contrast Security DevOps-Native AppSec Platform Benefits

- **Speed.** Provides real-time vulnerability analysis and threat telemetry
- **Accuracy**. Directly measures the risks in a running application
- **Scale**. Runs in parallel across any number of applications including open source
- **Process fit**. Aligns development and security operations
- **Cost**. Unburdens security staff while reducing operating expenses (OpEx)

"The saying 'you can't manage what you can't (or don't) measure' has never been more true than in the implementation and maintenance of DevSecOps." [2]

[1] "2019 Data Breach Investigations Report," Verizon, April 2019.
[2] "The Six Pillars of DevSecOps," Cloud Security Alliance, August 7, 2019.

Contrast SECURITY

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