Contrast Assess

Interactive Application Security Testing (IAST) Solution

CHALLENGES

- *Traditional static and dynamic application security tools are an impediment in today's high speed Agile DevOps environments.*
- *Open source software applications are becoming even more vulnerable and exposed to compromise making them attractive targets for attack.*
- *In the Verizon Annual Data Breach Report, web application attacks are the #1 source of data breaches.*
- *In the Gartner research report, 84% of breaches exploit vulnerabilities in the application layer.*

SOLUTION

Contrast Assess is an innovative, automated application security testing solution that infuses software with vulnerability assessment capabilities so that security flaws are automatically identified.

Leveraging a well-known industry methodology known as deep security instrumentation, Contrast Assess operates unobtrusively during development and testing of web applications or APIs. This passive approach to security testing eliminates the need for time-wasting and ineffective static security scans.

Contrast Assess provides continuous vulnerability assessment that integrates seamlessly with existing software development life cycle (SDLC) processes scaling across the entire application portfolio.

DIFFERENTIATORS

Our unique approach to modern application security produces the real-time intelligence and continuous visibility necessary to detect and remediate vulnerabilities with virtually no false positives or false negatives.

Ideal for Agile, DevOps, and DevSecOps

Contrast Assess is purpose-built from the ground up to work interactively with developers as they write and test web applications and APIs. DevOps teams can use Contrast with their standard messaging and build tools, automated provisioning systems and containers such as Slack, Maven, and Docker, to discover and report on vulnerabilities within an application. Contrast Assess automatically provides security analysis during automated tests and can be integrated with a CI/CD automation server, such as Jenkins, to fail a build that has excessive vulnerabilities.

Continuous Analysis

Contrast Assess uses deep security instrumentation to produce accurate vulnerability analysis. Development, QA, and Security teams get real-time results as they develop and test software, enabling them to find and fix security flaws early in the SDLC when they are easiest and cheapest to remediate.

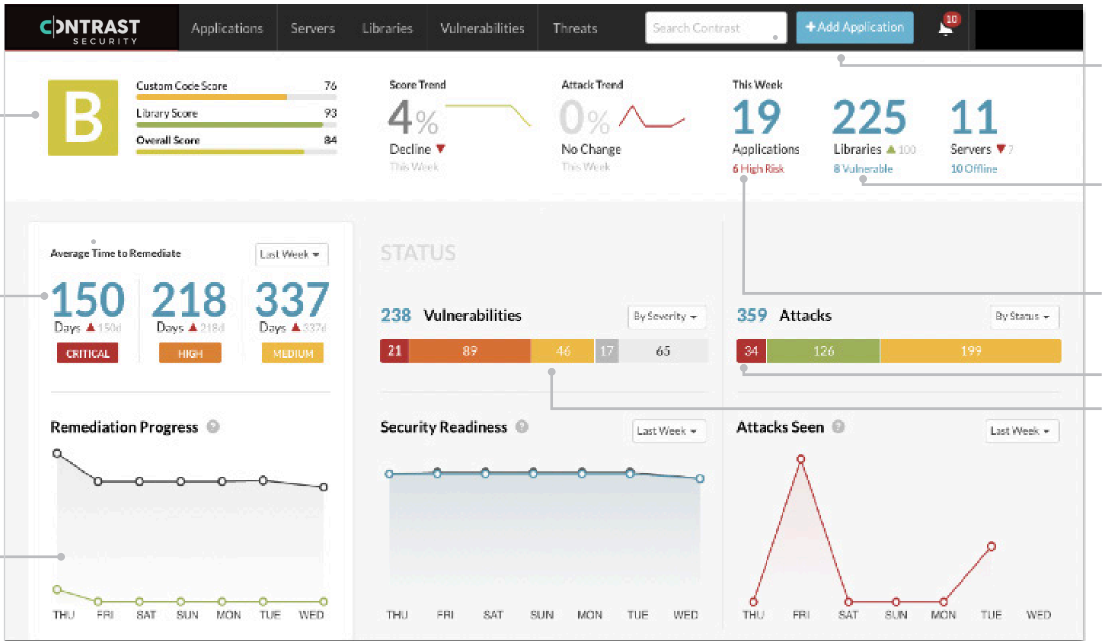
Highest Accuracy

Unlike legacy application security testing tools, Contrast Assess produces accurate results that developers can immediately act upon. This is due to the automation and visibility Contrast Assess has into the application and its runtime environment. It fuses together the most effective elements of IAST, SAST, and DAST application security testing approaches, with configuration and open-source security analyses, and delivers them directly into applications.

Scalable Architecture

Contrast Assess scales, since it instruments application security into each application, delivering and distributing vulnerability assessment across an entire application portfolio. Every running application continuously produces results in parallel.

TeamServer Management Console



Overall Grade & Score

STATUS:
Average Time to Remediate

Timeline Charts

Application Language Java,
.NET, Nodejs, Ruby

Library Analysis for Each
Application:
- Versions in use
- Classes of each library
- Number of CVEs

# of Apps, # Libraries, # Servers

Apps Being Attacked

Level of Vulnerability
(Critical, High, Medium)

KEY FEATURES

Contrast Assess Architecture consists of two main components:

1) Agents that run alongside the application on the application server and perform vulnerability assessment.
2) A centralized management console (TeamServer) that collects and reports on vulnerabilities identified by the agents and controls the deployment.

Extensive Vulnerability Coverage

Contrast provides extensive coverage over the most common application security risks, including the OWASP Top Ten.

Code-Level Remediation Advice

Contrast's innovative security trace format pinpoints exactly where a vulnerability appears in the code, and how it works. Contrast "speaks the developer's language," providing remediation guidance that is easy to understand and implement.

Third-Party Code Analysis

Like icebergs, 80% of the code in modern applications is "beneath the surface," lurking in libraries, frameworks, and other components. Applications often have 50 or more of these libraries, comprising millions of lines of potentially vulnerable code.

Application Inventory

Though it may appear simple, application inventory may be the hardest problem to solve for application security teams. Organizations may have hundreds or thousands of applications, Microservices, APIs – each with multiple instances of different versions installed across development and QA – and they're all constantly changing. Contrast tracks and continuously feeds information about internal and external web services, and their relationships across an application into a unified security inventory and bill of materials that's always up-to-date.

Live Application Architecture

Contrast automatically generates simple diagrams that illustrate the application's major architectural components. This information helps the developer quickly identify the meaning of a vulnerability.

CONTRAST
SECURITY
240 3rd Street
Los Altos, CA 94022
888.371.1333

Contrast Security is the world's leading provider of security technology that enables software applications to protect themselves against cyberattacks, heralding the new era of self-protecting software. Contrast's patented deep security instrumentation is the breakthrough technology that enables highly accurate assessment and always-on protection of an entire application portfolio, without disruptive scanning or expensive security experts. Only Contrast has sensors that work actively inside applications to uncover vulnerabilities, prevent data breaches, and secure the entire enterprise from development, to operations, to production.

7/15/19