Contrast SECURITY

SOLUTION BRIEF

Contrast Assess with Interactive Application Security Testing (IAST)

Executive Overview

Traditional approaches to web application security (AppSec) that rely on scanning lines of code for known vulnerabilities lack visibility and accuracy. As a result, they depend on manual security checks by expert staff to triage and interpret the results before handing recommendations with limited context back to developers to fix the problems. This inefficiency inhibits development cycles, increases costs, and often fails to eliminate many vulnerabilities that can be exploited by cyberattacks.

To avoid these issues, Contrast Assess uses instrumentation to embed security directly into the development pipeline. It automatically identifies and diagnoses software vulnerabilities in applications and application programming interfaces (APIs), thereby enabling organizations to release secure software to end users faster and with fewer risk exposures. Plus, it offers the broadest language support in the industry among interactive application security testing (IAST) solutions.

Traditional Testing Tools Miss Too Many Critical Vulnerabilities

Many AppSec solutions, such as static application security testing (SAST) and dynamic application security testing (DAST), promote a false-sense of security. They either scan an application's source code or use brute force attacks to find vulnerabilities. As a result, their outside-in approach lacks awareness of the full application context, leading to both false positives and false negatives. These inaccuracies create noise that interferes with effective prioritization of vulnerabilities—increasing an application's risk posture.[2]

These legacy AppSec tools are also slow and require experts to manage and significant infrastructure investment to deploy. They depend on the security staff to manually triage and interpret "noisy" results. These are then returned back to development teams (often in the form of a PDF list) without the full context of the vulnerability nor prioritization. As a result, developers spend valuable time tracing the root cause of the vulnerabilities and then verifying successful remediation. This creates friction between two teams that have distinctly different priorities and major business objectives (MBOs).

> *"One out of four data breaches last year were the result of attacks that exploited web application vulnerabilities.[1]*

Contrast SECURITY

Software developers need AppSec that is built for the dynamic and modularized nature of modern applications, enabling them to analyze data flow within applications and through APIs. They also need to reduce time to market by detecting vulnerabilities earlier in the software development life cycle (SDLC). Perhaps most importantly, as false positives create alert fatigue, developers need to eliminate the noise through accurate detection and prioritization of vulnerabilities for fast and effective remediation.

Instrumentation-Based Security Boosts Visibility and Accuracy

Contrast Assess automatically identifies and diagnoses software vulnerabilities in applications and APIs by using instrumentation to pinpoint and prioritize software vulnerabilities. By embedding sensors inside applications, organizations can "shift left" and discover vulnerabilities earlier in the SDLC.

This approach provides the highest accuracy, efficiency, and coverage possible. Contrast Assess enables companies to significantly decrease security team triage and DevOps remediation expenses. In addition, reducing alert noise (caused by false positives) helps eliminate hours of work required of DevOps teams to find and fix vulnerabilities without in-depth understanding of a specific vulnerability's priority. Instrumentation is the key to transforming AppSec into a continuous process. Contrast Assess increases security visibility across the application attack surface while transforming security from a checkbox that requires special expertise into something that occurs while they are writing code—all without any extra security expertise.

Continuous Assessment for Modern Software

Contrast Assess uses real-time intelligence and continuous visibility to quickly detect and remediate problems with virtually no false positives or false negatives. It was purpose-built for today's DevOps environments, making it easier to detect, prioritize, and fix critical vulnerabilities as developers test and write code. Contrast Assess also supports more languages than any other IAST solution available today—including Java, Node, .Net, Ruby, and Python.

SAST solutions can see the code, but they make a lot of assumptions about how functions are called and how data flows through an application. Black-box DAST solutions just see the HTTP endpoints and do not understand how requests are actually processed. Instead, Contrast Assess was designed for modern software architectures and deployment models, including microservices, APIs, and cloud-native applications. As a core component in Contrast's DevOps-Native AppSec Platform, it helps provide protection across the entire lifecycle of

> *"Existing approaches to AppSec are ineffective. The number of critical exposures per application remains the same today as it was 20 years ago—26.7 serious vulnerabilities.*[3]

Contrast SECURITY

the application—transparent, continuous software vulnerability assessment across all executed code. Further, though Contrast Assess' core capabilities center around IAST, it also leverages static and dynamic capabilities for specific findings.

The solution's sensor-driven assessment continuously monitors all parts of the application stack for vulnerabilities. Contrast Assess then instantly alerts of any findings, empowering developers to identify, fix, and verify remediations during runtime—providing an "always-on" security assessment. Because it is embedded in the software, it runs anywhere the application runs—including integrated developer environments (IDEs), on a local testing server, on a quality assurance (QA) machine, part of the continuous integration/continuous deployment (CI/CD) build, in a container, or in the cloud.

Security at Devops Speed that Boosts Time to Market

The accuracy and ease of use of Contrast Assess helps organizations detect and fix threats earlier in the CI/CD pipeline. This is important because it costs six times more to fix a bug found during implementation than to fix one identified during design; 15 times more if it is identified in testing; and 100 times more during regular maintenance once the code is in production.[4] In this pursuit, Contrast Assess empowers DevOps teams to write cleaner code during development while enabling aggressive delivery schedules and dramatically reducing security incidents in production.

Contrast Assess offers a replacement for traditional application security because it diagnoses data flows and analyzes requests and responses. Its patented instrumentation technology interrogates application frameworks to determine all possible data routes. It automatically discovers the entire attack surface, prioritizes remediation efforts, and accounts for parameters like service level agreements (SLAs) for code releases.

Elastic Scalability that Conserves Resources

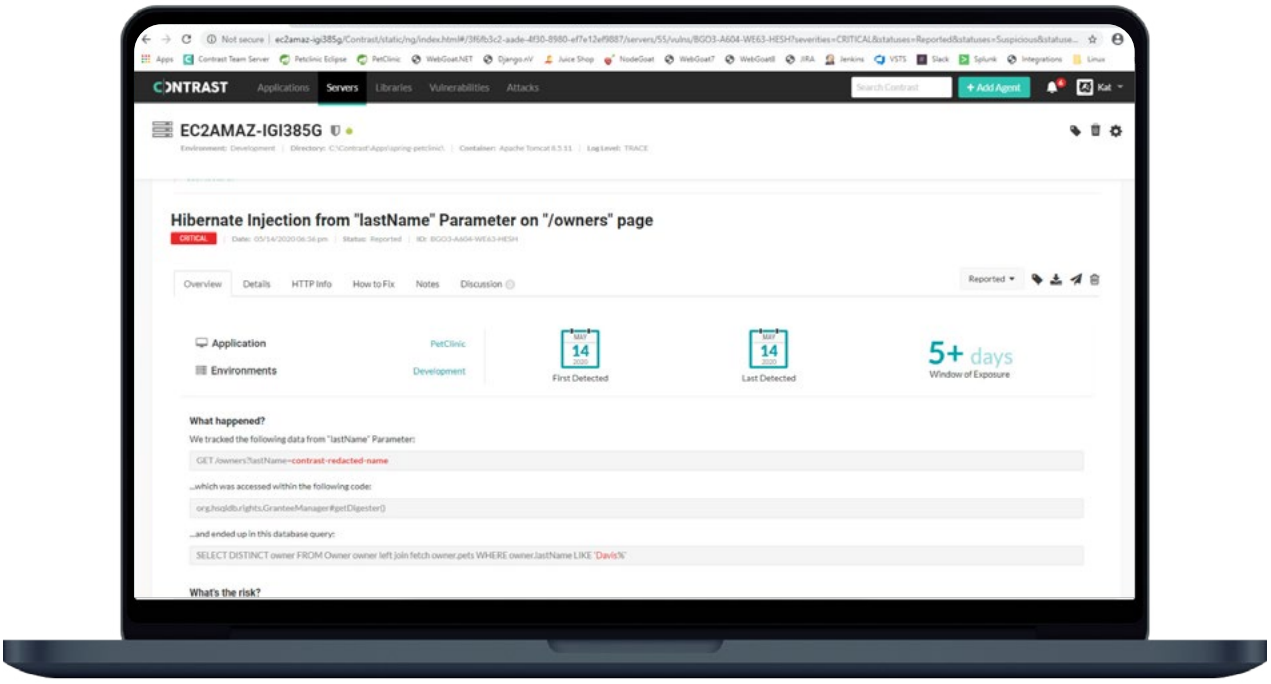
Contrast Assess is fully distributed and able to continually assess thousands of applications in parallel. This eliminates the need for an army of security experts and enables businesses to expand their application offerings without security becoming a bottleneck.

The solution also accelerates application workflows through impactful collaboration between development and security and operations (enabling a true DevSecOps model). It creates an instant feedback loop, providing developers with immediate and continuous threat vulnerability visibility. This helps organizations save both time and money in development.

> *By deploying comprehensive DevSecOps automation, organizations gain visibility and control over the development life cycle, along with a closed-loop pipeline for testing, reporting, and solving for potential security concerns.*[5]

Contrast SECURITY

Contrast Assess also supports new regulatory and compliance guidelines that acknowledge how legacy application security tools are unable to address today's advanced threat landscape. National Institute of Standards and Technology (NIST) 800-53, Payment Card Industry Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), PCI Security Framework, and Open Web Application Security Project (OWASP) Top 10 specifically call out IAST as an essential technology for combating modern software threats in today's modern software era.



Contrast Assess Accelerates Secure Application Development

Contrast Assess provides a highly accurate, scalable, and ideal solution for modern DevOps environments that require quick time to market. It enables visibility of data flows across the entire application stack and reduces the noise of false positives while helping development teams prioritize which parts of the application should be immediately fixed. This helps organizations align security and development processes, eliminate manual security workflows, and accelerate the release of new applications.

[1] "2019 Data Breach Investigations Report," Verizon, April 2019.
[2] Augusto Barros, "From my Gartner Blog – Considering Remediation Approaches For Vulnerability Prioritization," Security Boulevard, May 2, 2019.
[3] "Malware and ransomware attack volume down due to more targeted attacks," Help Net Security, February 5, 2020.
[4] Mukesh Soni, "Defect Prevention: Reducing Costs and Enhancing Quality," iSixSigma, accessed April 16, 2020.
[5] "How to Leverage DevOps and Automation to Bolster Security," Tripwire, July 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