Contrast SECURITY

Bump Fists Not Heads:

SECURITY AND DEVELOPMENT TEAMS CAN WORK BETTER TOGETHER WITHOUT SECURITY DELAYS

Legacy approaches to application security (AppSec) not only deliver inadequate protection across the software development life cycle (SDLC) but they also create unacceptable bottlenecks for developers who face constant pressure to meet aggressive timelines. The delays caused by running frequent security scans, manually finding and remediating vulnerabilities, and sifting through numerous alerts can make developers feel as if they are constantly "butting heads" with the security team.

Go From Butting Heads to Bumping Fists

Following are some of the most prevalent ways in which the Contrast DevOps-Native AppSec Platform eliminates development roadblocks and enables security and development teams—who are often at loggerheads over conflicting objectives and measurements—to go from butting heads to "bumping fists."

MAKING SECURITY SCANS A THING OF THE PAST

Frequent scans—and the related manual vulnerability interventions security teams mandate—consume valuable time for developers and slow development cycles. Contrast Security instrumentation embeds continuous vulnerability scanning into the application itself using Contrast Assess and Contrast OSS. This eliminates frequent scans by legacy tools such as static application security testing (SAST), dynamic application security testing (DAST), and software composition analysis (SCA)—which can interrupt development for hours at a time.

DELIVERING CONTINUOUS, REAL-TIME FEEDBACK

Legacy tools only provide feedback when scans are executed. Continuous feedback from Contrast Assess and Contrast OSS delivers actionable, code-level feedback that enables developers to remediate vulnerabilities on the fly—before they can cause delays to coding. Security teams are satisfied because they have transparent visibility into the full application attack surface and real-time vulnerability status.

SIMPLIFYING VULNERABILITY REMEDIATION

Feedback from SAST and DAST tools is often inadequate for developers to locate and fix a vulnerability without manual research. With Contrast Security instrumentation, developers no longer need to sort through code to find the source of a vulnerability. Route Intelligence in Contrast Assess provides the URL of the route through which the vulnerability can be accessed, making remediation easy and quick.

Contrast SECURITY

AUTOMATING REMEDIATION VERIFICATION

With legacy tools, verification of fixes to vulnerabilities is a manual process that sometimes requires another time-consuming scan. But because it continuously scans software throughout the SDLC, instrumentation in Contrast Assess, Contrast OSS, and Contrast Protect provides immediate feedback as to whether a vulnerability fix was successful. This eliminates another legacy manual process that has long frustrated developers, while assuring the security team that vulnerabilities are being addressed

ADDRESSING OPEN-SOURCE VULNERABILITIES THAT REALLY MATTER

Legacy SCA tools simply provide a list of vulnerabilities detected, without any prioritization or analysis. Contrast OSS goes far beyond this by continuously cataloging and reporting library contingencies and prioritizing vulnerabilities according to risk. The tool omits vulnerabilities that are present in code but not actually used at runtime, saving developers time in remediating items that pose no risk while providing the security team with visibility and verification.

ELIMINATING TIME-WASTING ALERT FATIGUE

As SAST and DAST tools have a high percentage of false positives, developers spend a lot of time sifting through irrelevant alerts, even though they are measured on how much code they can write and how fast they can release it. Web application firewalls (WAFs) that protect applications in production are also notorious for false positives, and developers can be pulled off current projects to chase these dead ends. Because Contrast Security virtually removes false positives through security instrumentation, developers can focus on vulnerabilities that can be exploited. This saves significant time for developers while eliminating a frustration felt by the security team.

CATCHING VULNERABILITIES EARLIER WITH MORE COMPREHENSIVE SCANNING

Legacy, signature-based AppSec tools are also notorious for false negatives and missed vulnerabilities, which can cause even more delays and security issues than false positives. Developers can be pulled off new projects for emergency remediation on old ones, and security teams face the prospect of successful attacks in production. Contrast Security uses continuous scanning that analyzes the application using multiple datasets—including Route Intelligence, which analyzes the “routes” taken by real users of the application. This virtually eliminates false negatives and enables developers to detect vulnerabilities earlier in the timeline, when they are less costly and time-consuming to remediate.

Contrast SECURITY

AUTOMATING SECURITY FOR APPLICATIONS IN PRODUCTION

It is not uncommon that vulnerabilities missed by SAST and DAST tools are ultimately exploited in production, as WAFs are signature-based and notorious for false negatives. This can create a huge time sink for both developers and security team members. Contrast Assess delivers secure applications for production, and Contrast Protect enables applications to be self-protecting after being released. This removes the need for developers to be pulled off current projects for emergency remediation on a past project, while enabling security team members to focus on more strategic priorities.

IMPROVE COORDINATION WITH SECURITY TEAMS— WHILE REDUCING INTERACTIONS

Traditional AppSec creates multiple roadblocks for efficient development teams that are simply trying to do their jobs. Rather than “butting heads” with the security team because of frustrations over coding delays, Contrast Security enables developers to “bump fists” with them. The two teams no longer work at cross-purposes, but rather can work together to deliver secure applications on aggressive timelines. And this can take place while reducing time-consuming interactions between the teams, as developers can deal with the vast majority of vulnerabilities themselves. This creates a collaborative relationship that enables both teams to focus on what they were hired to do.

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