Contrast SECURITY

SOLUTION BRIEF

Contrast Security Integration

with CI/CD Pipelines

Executive summary

The Contrast Application Security Platform helps eliminate vulnerability remediation bottlenecks by integrating security testing with the existing tools and workflows that developers use in their DevOps and Agile environments. This includes ensuring verification within popular continuous integration/continuous deployment (CI/CD) tools such as Jenkins and Azure DevOps. Contrast CI/CD integration ensures that vulnerable or noncompliant applications are not promoted to production.

CI/CD tools need integrated application security

Developers have turned to CI/CD tools like Jenkins and Azure DevOps to help expedite the creation of new applications and meet increasingly rapid delivery cycles. While CI/CD tools help accelerate delivery, a lack of integration with application security means that very often developers are pushing vulnerable builds to production. And this problem is widespread—the percentage of data breaches tied to application vulnerabilities doubled over the past year to account for 43% of all reported incidents.[1]

Lack of CI/CD integration creates a number of problems. Application security managers have difficulty in getting developers across business units and application teams to adopt the same criteria for failing builds. This leads to "cheating"—where developers may increase the number and types of allowed vulnerabilities in a build in order to meet deadline pressures. It becomes impossible for application security to enforce policies if vulnerabilities are reported after builds are released. And for developers, traditional application security solutions that operate in their own silos cannot provide vulnerability information at a time when they can efficiently do something about it in terms of remediation.

> To build a secure DevOps program that automates cybersecurity processes and controls via integration with the CI/CD delivery toolchain, organizations must shift security left into development and build times.[2]

In order to address these problems, application security must become an integrated part of existing CI/CD toolchains so that vulnerabilities can be fixed in real time, like any other problem in an application build.

The contrast application security platform

The Contrast Application Security Platform integrates with CI/CD tools such as Jenkins, Azure DevOps, CircleCI, and Bamboo. Contrast's solutions include Contrast Assess interactive application security testing (IAST), which identifies software vulnerabilities in custom code, and Contrast OSS to ensure security of open-source components. The Contrast Application Security Platform also includes Contrast Protect runtime application self-protection (RASP).

Contrast SECURITY

This instrumentation-based approach to application security testing simplifies the development toolchain and streamlines workflows. Contrast provides detailed contextual information such as data-flow analysis as well as actionable fix guidance to help developers efficiently find and remediate critical vulnerabilities at the same time that they address all other issues in a broken build. This helps developers improve the security of their code while eliminating the back-and-forth dependency on application security analysts that bog down delivery cycles.

CI/CD integration—security verification at devops speed

Contrast's integration into CI/CD processes enables application testing to be automatically embedded into the pipeline to achieve much greater agility. It coordinates the objectives of both security and development teams within existing CI/CD tooling for greater efficiency and productivity. At the same time, it also helps organizations ensure that critical vulnerabilities don't reach production.

Toolchain complexity can weaken security—and nearly half (45%) of IT professionals report difficulty ensuring security across the toolchain.[3]

CONTRAST INTEGRATION CAPABILITIES

The Contrast platform allows policies to be centrally created and managed by the application security team for greater control over standardization of pipeline failure criteria. In Jenkins, for example, Contrast integration allows management to set parameters for build classifications (e.g., unstable, fail) across the entire development organization while enabling consistent build parameters. Vulnerable builds or deployments can be blocked and alerts can automatically be sent if critical vulnerabilities are found in a failed or unstable build. Contrast also offers analytics and reporting by type and by build in Jenkins.

CONTRAST BENEFITS TO APPLICATION SECURITY

Contrast's approach offers benefits to application security teams, including:

- Putting remediation in the hands of developers while eliminating critical application vulnerabilities
- Consistent enforcement of policy for improved efficiency, consistency, and greater control
- The ability to be immediately alerted if a build introduces a vulnerability and/or automatically sets builds to fail when a new vulnerability is found
- Better visibility and control over what is published in production

Contrast SECURITY

CONTRAST BENEFITS TO DEVELOPERS

Contrast integration with CI/CD tooling also offers substantial benefits for developers, such as:

- Improving developer productivity and their ability to plan their time
- Increasing the amount of quality time available to spend on coding
- Eliminating context switching and unplanned work interruptions
- Decreasing the total time spent on vulnerability remediation per application
- Helping organizations "shift left" by fixing vulnerabilities in development, rather than later in the software development life cycle (which is more expensive)

DRIVING REMEDIATION, ACCELERATING DEVSECOPS

The Contrast Application Security Platform integrating with existing tools allows development, operations, and security teams to synchronize efforts for greater efficiency, productivity, and protection. Automating cybersecurity processes and controls via integration with the CI/CD toolchain that orchestrates the application life cycle defines a true DevSecOps model.[5]

Contrast integration gives application security managers the ability to set and enforce policies to ensure that vulnerable applications do not get promoted to production. At the same time, it also helps developers work more efficiently to deliver high-quality code and still meet aggressive delivery schedules. It simultaneously improves the speed and quality of development while freeing up valuable team resources to focus on strategic execution and future innovations.

> The cost to fix an error found after product release was four to five times as much as one uncovered during design, and up to 100 times more than one identified in the maintenance phase.[4]

Contrast SECURITY

[1] "2020 Data Breach Investigations Report," Verizon, June 2020.
[2] Veronica Combs,"DevOps needs to morph into DevSecOps to close security threats in the cloud," TechRepublic, May 14, 2020.
[3] "Modernize your CI/CD," GitLab, accessed December 21, 2020.
[4] Mukesh Soni,"Defect Prevention: Reducing Costs and Enhancing Quality," iSixSigma, accessed December 14, 2020.
[5] "Oracle and KPMG Cloud Threat Report 2020," Oracle/KPMG, May 2020.

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