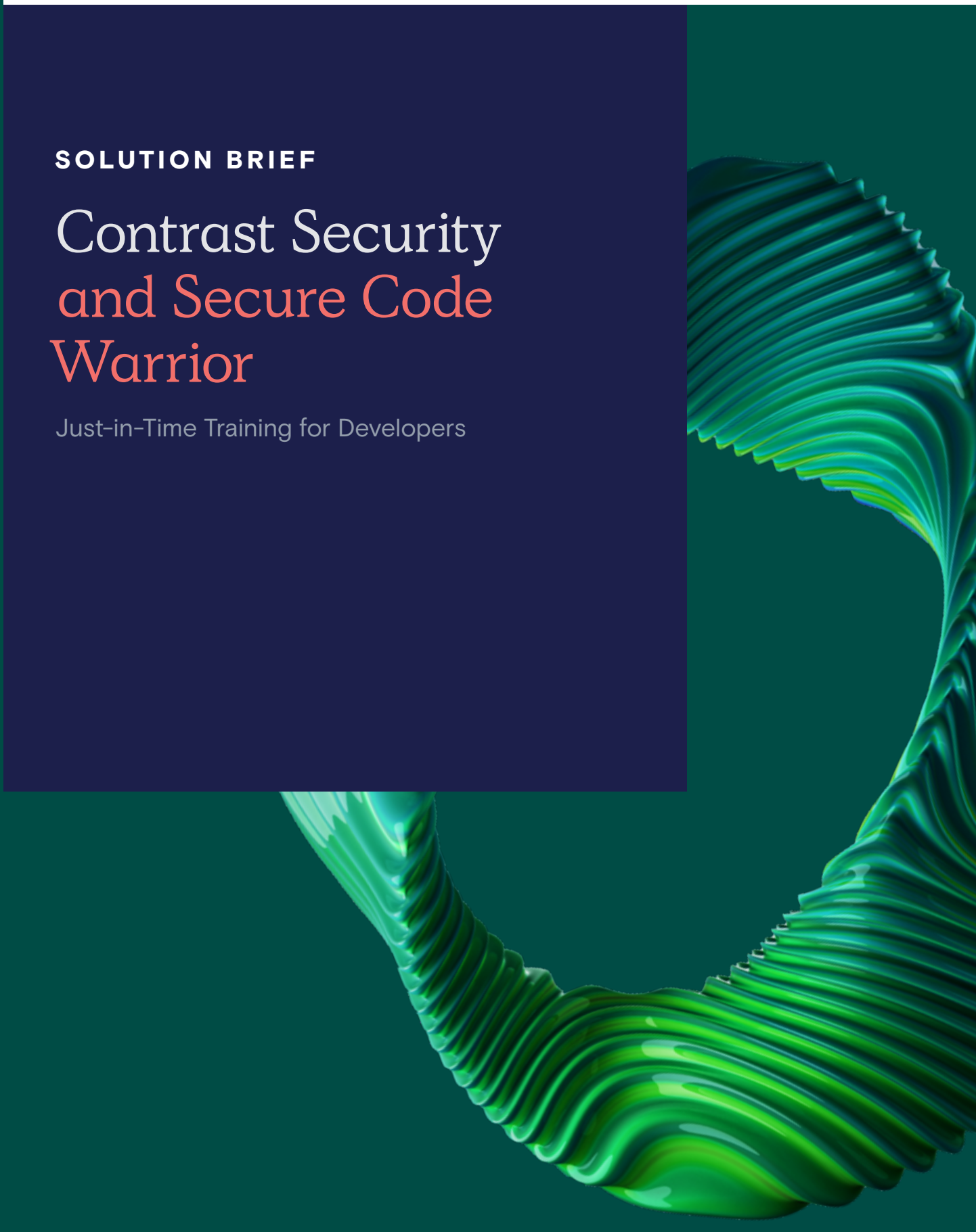
Contrast SECURITY

SOLUTION BRIEF

Contrast Security and Secure Code Warrior

Just-in-Time Training for Developers



Executive summary

Today, developers are under ever-increasing pressure to do more and to do it faster. The move to Agile and DevOps environments and new digital tools helped accelerate software delivery schedules. However, the limitations of traditional application security testing (AST) tools and a shortage of security experts to analyze results force many developers to choose speed over security. At the same time, traditional security training methods cannot scale to keep up with the ever-accelerating churn of modern continuous integration/ continuous deployment (CI/CD) pipelines. For application security to keep pace, developers need help remediating vulnerabilities on their own.

Contrast Security and Secure Code Warrior deliver an industry-leading, just-in-time training approach that empowers developers to learn secure coding as they write and release applications. This integrated solution combines runtime vulnerability detection and line-of code level remediation guidance with dynamic learning tools. This joint solution helps

developers gain the necessary security skills to ship secure software at speed.

The Need for Modern Devsecops Training

A recent study reported the vast majority (79%) of developers are under pressure to shorten development cycles—releasing code to production multiple times per week. But at the same time, 85% admit that their average application has 10 or more vulnerabilities.[2] Businesses with more security debt across their portfolios fall farther behind and experience escalating volumes of vulnerabilities—1.7x higher than for organizations with below-average security debt.[3]

This problem persists for three main reasons:

- First, traditional AST tools are highly inaccurate because they were not designed for modern development environments. High volumes of false positives yield noisy test results.

> *According to Verizon's 2021 Data Breach Investigations Report, 39% of all data breaches last year can be traced back to an application vulnerability.[1]*

Contrast SECURITY

- To compound the previous issue, organizations also cannot hire enough security specialists to triage and analyze the noisy testing results. Security teams must sift through piles of alerts and determine which ones are true vulnerabilities and which ones are false positives before giving the results to developers for remediation. The growing shortage of application security specialists makes qualified staff hard to find, hire, and retain.[4] Reliance on limited human security resources bottlenecks workflows and can delay releases. Even if developers were to fix vulnerabilities, they cannot do so. Most traditional AST solutions offer very little automated guidance to help developers find and fix their own vulnerabilities. The limited support that is provided is usually not written with the developer in mind—lacking the necessary context or depth of detail to provide "line-of-code" level remediation instructions. Subsequently, vulnerabilities get ignored or simply do not get fixed before the delivery deadline.

- The third key problem is the limitations of traditional security training methods for developers. Legacy application security training typically depends on a conceptual, point-in-time approach to educating developers. Most training tools today do not provide a positive and engaging experience because they cannot provide developers with just-in-time training that scales in line with aggressive CI/CD pipeline demands. And because training is not automatically tailored to fix the specific vulnerabilities detected in testing, developers often struggle with slow remediation processes. In addition, because learning is not reinforced, similar vulnerabilities may be reintroduced in future code segments.

> *A concerted effort to remediate the vulnerabilities that put businesses at risk and "pay down" the security debt of unremediated vulnerabilities is the single most powerful action a company can take to reduce the chance of a breach.*[5]

Security skills and automation are the foundation for achieving DevSecOps across the enterprise. If organizations are going to promptly write and release code with fewer vulnerabilities, they must empower their developers to be part of the solution. And developers want to release secure code—in fact 77% of them say they want more training in application security to help improve the quality of their applications.

Secure Code Warrior and Contrast have joined forces to address this specific need.

Contrast SECURITY

Helping Developers Write Secure Code—Faster

The integrated solution from Contrast Security and Secure Code Warrior delivers industry-leading just-in-time contextual security training and augmented "how-to-fix" guidance. The joint approach is designed to enhance a developer's ability to fix application vulnerabilities themselves without assistance from the security team. Vulnerability-specific training tools are automatically embedded into the integrated development environment (IDE), CI/CD tools, and within the Contrast UI.

Contrast Assess and **Contrast OSS** eliminate security bottlenecks from application development, reduce the noise of false positives, and scale modern security capabilities across the software development life cycle (SDLC). Contrast's approach uses binary code instrumentation to monitor, test, and report from inside the application itself. For each vulnerability detected, the Contrast platform provides developer-friendly guidance for finding and resolving the issue—without involving a security expert. Contrast's innovative Security Trace format pinpoints exactly where a vulnerability appears in the code and explains how it works.

Secure Code Warrior provides a platform for developer learning pathways with code-specific challenges, interactive missions, micro-learning videos, and engaging tournaments. With respect to this joint solution, contextual micro-learning from Secure Code Warrior is embedded in the Contrast UI "How To Fix" section for each vulnerability finding. Developers can view training modules on a specific vulnerability, or click on the language reference link to go to a code-specific exercise. Additionally, this information can be accessed via all Contrast IDE plugins (e.g., Eclipse, Maven, VS Code). A third option is also available with a Jira integration plugin managed by Secure Code Warrior.

A JOINT SOLUTION WITH AMPLIFIED BENEFITS

The Contrast Security and Secure Code Warrior joint solution further enhances a developer's ability to fix vulnerabilities easily without the need of security expertise. Developers can elevate their security competencies as they write using context-aware, just-in-time learning materials that are specific to the vulnerabilities and code currently under remediation.

Through the Contrast and Secure Code Warrior integration, organizations can:

- Make security skill-building efforts for developers both relevant and just-in-time
- Improve the average time to remediate for vulnerabilities
- Reduce the number of new vulnerabilities introduced per build.

Security at the Speed of Devops

Developers need better security knowledge to commit cleaner, lower risk code with fewer vulnerabilities. The integrated security automation and skill-building capabilities offered by Contrast and Secure Code Warrior coordinate training videos and code-specific exercise labs that are specifically tailored to the vulnerabilities discovered in their AST reports.

This gives developers the just-in-time security knowledge they need to strengthen their secure coding skills in both the near and long term. It promotes faster remediation and reduces the number of vulnerabilities that slip into production. This helps organizations "shift left" and reduce costs, since fixing a vulnerability gets more expensive as the development process gets further from where the error was introduced.[6]

Contrast SECURITY

[1] "2021 Data Breach Investigations Report," Verizon, May 2021.
[2] "Priorities and Challenges for Modern Software Developers," Contrast Security, October 2020.
[3] Katharine Watson, "Application Risk Is 1.7x Higher for Organizations That Fail To Manage Security Debt," Contrast Security, July 24, 2020.
[4] Jon Oltsik, "The cybersecurity skills shortage is getting worse," CSO, August 21, 2020.
[5] Yaniv Bar-Yadan, "How To Get Out Of Security Debt," Forbes, September 3, 2020.
[6] Jeff Williams, "How To Start Decluttering Application Security," Forbes, January 27, 2021.

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