EBOOK

Contrast SECURITY

Pipeline-Native Static Analysis: Why It Is The Future Of Sast

Executive Overview

Traditional application security scanning is based on decades-old scanning models that lack the capabilities to discern actual threats from a sea of probes that blindly search for any chance to exploit an application. These testing tools are slow, deliver inaccurate results, and lack contextual guidance to help developers fix their own code issues in real time.

Organizations need modern scan-based testing—a pipeline-native approach that integrates into DevOps/Agile workflows, tooling, and systems. An effective solution should harmonize the objectives of development and security teams to enable both faster development cycles and higher-quality code at the same time.

> More than half (55%) of developers admit to skipping security scans in order to meet deadlines.[1]

[1] "The State of DevSecOps Report," Contrast Security, December 2020.

Table of contents

01

The Problems with Outdated Security Scanning Tools

The scanning tools used for application security testing in most development environments today are long out of date. They were not designed with modern DevOps or Agile processes in mind—and therefore, they bring a number of critical liabilities to organizations:

Traditional scanning tools are slow, compute intensive, and expensive. The vast majority of organizations (91%) say that vulnerability scans take at least three hours—and for 35%, they take eight or more hours.[2] Once the scan report is generated, it takes the application security team an average of one hour to triage and diagnose each alert. For those that are true vulnerabilities, over half of developers spend more than four hours locating the cause of the vulnerability and fixing it. Even once a vulnerability is fixed, individual developers admit they spend six hours per week verifying that their remediation efforts actually fixed the issue and they didn't introduce a new flaw into the code.

> Fixing a vulnerability gets more expensive as the development process gets further from where the error was introduced—and for one major application security vendor, the average MTTR is currently 171 days.[3]

[2] "The State of DevSecOps Report," Contrast Security, December 2020.

[3] Jeff Williams, "How To Start Decluttering Application Security," Forbes, January 27, 2021.

The “breadth” approach taken by incumbent scan-based application security solutions also bottlenecks DevOps processes. Traditional static application security testing (SAST) solutions look for large sets of code quality and/or security-related issues across all parts of the codebase, regardless of the parts of the application that are executed at runtime. Exercising every line of code (regardless of the actual risk it presents) results in a large rule set and consequently a longer, compute-intensive scanning process. Subsequently, organizations can be hampered from shipping applications on time, or they are incentivized to skip security testing—which increases risk of critical code vulnerabilities in production.

Noisy results obstruct prioritization and mitigation. Traditional scanning solutions also attempt to build a model of an application in order to project the application’s runtime behavior (and subsequently the vulnerabilities in it) that results in many false positives. With as many as 85% of alerts being false positives, noisy results cause alert fatigue among staff.[4] Further, SAST inaccuracy means that teams often waste cycles addressing low-priority alerts while missing critical vulnerabilities that introduce real risks.

Since most security testing solutions are not present at runtime, they cannot provide risk prioritization ratings using application context and know which vulnerabilities are more likely to occur within that application. Teams struggle to correlate, prioritize, and remediate potential application risks in scan results—which causes developer frustration. As a result, developers often waste time on vulnerabilities that pose no risk at all. Critical problems may not get fixed in a timely manner—or they may be missed entirely and make their way into production.

Adding more security personnel to manage alerts and analysis isn’t a practical answer. The worsening shortage of application security specialists makes qualified staff hard to find, hire, and retain.[5] With the number of hours spent running scans and assessing results growing at the same time, application security simply cannot scale. And this limitation ultimately hamstrings an organization’s ability to develop and deliver new software.

> “The vast majority of organizations (73%) report that each security alert they receive consumes an hour or more of application security time.[6]

[4] “Digital Transformation Thwarted: When Your AppSec Tools, Scanning, and Resources Become Your Mr. Hyde,” Contrast Security Webinar, July 23, 2020.
[5] Jon Oltsik, “The cybersecurity skills shortage is getting worse,” CSO, August 21, 2020.
[6] “The State of DevSecOps Report,” Contrast Security, December 2020.

Lack of developer-friendly remediation guidance. Most of today's security testing solutions do not offer appropriate guidance that could help developers fix vulnerabilities without the involvement of security experts. Guidance is typically limited, not written with the developer in mind, and does not offer contextual detail for "line-of-code" level instructions. In addition, the mode of operation for most of these solutions does not fit into the development workflow—these solutions don't integrate with DevOps-native tooling such as ticketing systems, chat tools, or continuous integration/continuous deployment (CI/CD) pipelines.

> "A concerted effort to remediate the vulnerabilities that put businesses at risk and "pay down" their security debt (VIZ., An increasing number of unremediated vulnerabilities) is the single most powerful action a company can take to reduce the chance of a breach.[7]

[7] Yaniv Bar-Yadan, "How To Get Out Of Security Debt," Forbes, September 3, 2020.

02

The Need For Pipeline-Native Application Security Scanning

To support the speed and scale of DevOps/Agile environments, a modern, pipeline-native security scanning solution is focused, actionable, and fast.

Focus on Results that Matter

Organizations need to be able to focus limited staff resources on the critical vulnerabilities that matter. To achieve this, an effective scanning solution must first provide highly accurate results that focus on vulnerabilities that can lead to exploitation. A modern scanning solution should help teams:

- Work with a single set of results across all facets of application security—including application security testing (AST), software composition analysis (SCA), and runtime application protection and observability
- Focus remediation via high-confidence, risk-prioritized findings
- Effectively use context from static and runtime analysis plus production traffic to help guide and accelerate in-line remediation by developers

Results Must Be Actionable

To eliminate the co-dependent workflows that bottleneck development pipelines, pipeline-native scanning must also include developer-friendly "how-to-fix" guidance. Accurate results with contextual information are framed as simple code-level updates that not only tactically fix the problem at hand but also educate the developer to avoid the introduction of future vulnerabilities.

This allows development teams to immediately act without delays or the need for deep security expertise. This information should pinpoint exactly where a vulnerability appears in the code, and how it might be remedied.

These capabilities can further simplify team operations by:

- Offering seamless software development life cycle (SDLC) integrations into tools in the developer's workflow (e.g., build tools, supply chain management/source-code repositories)
- Lowering the initial deployment friction through a developer-oriented install experience (e.g., using a command-line interface [CLI] or package manager)
- Incorporating specific, code-level remediation guidance informed by static and runtime analysis
- Integrating with other tooling in the SDLC to provide a unified view of application risk

Results Must Be Delivered Fast

Finally, pipeline-native scanning must provide a step function improvement in scan time. Organizations need fast and accurate testing results so that security teams can focus on more strategic tasks, such as threat hunting. At the same time, developers need the ability to immediately fix vulnerabilities in real time as they write code—without waiting for security team input, subsequent context switching, and snowballing remediation backlogs.

Faster scanning allows organizations to:

- Fix issues earlier in the development pipeline (which reduces remediation costs)
- Improve overall security performance by focusing on exploitable flows in the application runtime
- Defer noncritical vulnerability remediation via mitigating controls (providing “air cover” in production as part of a broader security platform)

Contrast SECURITY

03

Relevant Solution
Use Cases

A modern scanning solution that integrates into a broader application security platform—featuring solutions such as interactive application security testing (IAST), SCA, and runtime application protection and observability—can address several relevant development use cases:

Client and server-side application coverage. Modern scanning provides client-side (JavaScript) coverage while a complementary solution (like IAST) delivers best-of-breed testing for server-side applications.

A path to DevSecOps. A modern scanning solution can offer organizations better security today, plus a pathway to a more comprehensive, instrumentation-based platform of solutions with protection across the full SDLC. This can help align the objectives of development and security teams to harmonize efforts, accelerate delivery cycles, and improve the quality of code—the ultimate goals of a true DevSecOps environment.

Policy-driven scanning, without compromising speed, accuracy, and pipeline fit. A unified application security platform that includes modern scanning eliminates the need for a stand-alone, traditional SAST tool. Application security that offers a single, coordinated system for compliance reporting simplifies auditing processes and helps reduce regulatory risks.

Security across the SDLC. By adding or improving application scanning via a more modern solution, organizations can find vulnerabilities earlier in the SDLC—saving time and money while delivering more secure code to production.

04

Modern Scanning in a Platform-Based Approach to Application Security

Traditional scanning tools were not designed for today's demanding application development processes. A more effective approach to scan-based testing is one that's part of an integrated application security platform—one that shares contextual information across all parts of modern applications and throughout all stages of the SDLC.

In sum, a modern scanning solution should:

- Provide a step function improvement in speed
- Focus on critical vulnerabilities that get applications hacked
- Offer developer-friendly "how-to-fix" guidance
- Install and integrate seamlessly into developer workflows

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