Contrast SECURITY

AppSec noise and fatigue by the numbers

How Runtime Security safeguards applications

Relying on traditional application security testing (AST) solutions like Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) too frequently leads to headaches and insecure web applications.

Applications are increasingly being targeted

The number of data breaches caused by an exploited vulnerability rose **180%** year-over-year.[1]

50% increase in zero days being exploited year-over-year.[2]

Less than **6%** of applications have no flaws.[3]

Application vulnerabilities are not being adequately addressed

55 days after a third-party library vulnerability fix is released, half of applications continue using the unfixed version.[4]

55

48% of third-party flaws and 41% of first-party flaws are not remediated within 12 months.[5]

Legacy AppSec solutions have high false-positive rates

For some tools and some languages, SAST's false-positive rate is over **68%**.[6]

NIST has found that SAST's false-positive rate is as high as **78%** for Java.[7]

Per the OWASP Benchmark, DAST tools have a false-positive rate of **82%**.[8]

A high false-positive rate slows down remediation efforts, as dealing with **240** issues requires a full week's worth of effort.[9]

Why are false positives so damaging?

Wasted time and remediation effort

Erodes trust in tooling, and can damage trust between security and developers

SAST and DAST take too long

DAST tools may need up to **4** hours to scan some critical applications.[10]

Mean time to remediation (MTTR) for some leading AST solutions is **298** days.[11]

41% of first-party flaws are not remediated within 12 months.[12]

The difference that Interactive Application Security Testing (IAST) brings

Up to **3x** faster remediation times[11]

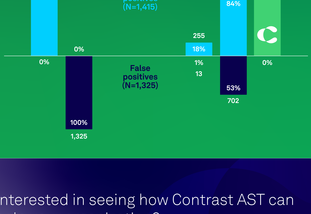
156% reduction in false positives.[12]

155% faster MTTR compared to leading AST solutions.[13]

Business benefits of IAST

Cost to triage all SAST/DAST results[14]	$60,394,464
Cost to triage all IAST results	$0

Contrast Security is the single best solution for optimizing for efficacy with a 100% true positive rate, per OWASP Benchmark.[15]



Interested in seeing how Contrast AST can help your organization?

Schedule a custom consultation today

[1] https://www.verizon.com/business/resources/reports/dbir/
[2] https://cloud.google.com/blog/topics/threat-intelligence/2022-zero-day-trends
[3] https://www.veracode.com/sites/default/files/2024-02/2024_the_gap1.2024_software_sec-0ovxLVqcGyOuTZEAAAGbbgZ0HE_cnpqwcAfmlaxHdmBE7y0dTpzGzfmTf3TSmyD6c9c2Bu9bNbDc2wZNNTYD7D5MDmqZ8YQ6p8pBuSz-hAMUjDqbgZ0NNJUEY
[4] Verizon DBIR
[5] 2024 Veracode State of Software Security Report
[6] https://personal.utdallas.edu/~ltw1453/publications/icst2016.pdf
[7] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-208.pdf
[8] https://owasp.org/www-project-benchmark/
[9] https://www.securitycompass.com/blog/safeguarding-software-quality-tackling-false-negatives-with-security-by-design/
[10] https://docs.veracode.com/r/getting-started-with-crawbless-security
[11] https://info.veracode.com/report-state-of-software-security-volume-12.html
[12] 2024 Veracode State of Software Security Report
[13] https://www.contrastsecurity.com/hubfs/customer-success/ssh.4
[14] ibid
[15] Contrast Security internal data, https://info.veracode.com/report-state-of-software-security-volume-12.html
[16] Results from one Fortune 100 Insurance Company from 2022
[17] https://owasp.org/www-project-benchmark/

All rights reserved. ©2024 Contrast Security, Inc.