CONTRAST SECURITY

EXECUTIVE BRIEF

A FALSE SENSE OF APPLICATION SECURITY

CYBER SECURITY BENCHMARK HIGHLIGHTS LEGACY PRODUCT FAILURES

Time to Choose a New Solution

In 2015, the Open Web Application Security Project (OWASP) Benchmark Project was created to measure the speed, coverage, and accuracy of application security products. The OWASP Benchmark Project lets organizations freely assess products they have or are planning to use. The results demonstrate conclusively that most organizations are operating with a false sense of security, and need to revisit their application security technology choice

Vulnerable Apps Remain the Biggest Cyber Security Threat

Companies spend billions of dollars every year on application security products, training, and consulting services to protect their applications from hackers and attacks. In spite of that investment, the 2016 Verizon Data Breach Report[1] found web applications were the number one source of successful data breaches over the last eight years. Clearly, something is not working according to plan.

1 Source: 2016 Verizon Data Breach Investigations Report, Figure 18

NEW BENCHMARK CONFIRMS DRAMATIC PRODUCT FAILURES

Security professionals have long believed that one of the main challenges with securing applications was the application security products available to them, but until now they had no way to prove it conclusively.

In 2015 OWASP published an open source Benchmark Project on application security testing accuracy. The Benchmark Project allows organizations to measure the effectiveness of application security testing solutions by providing an application with over 21,000 test cases across 11 different vulnerability categories. It also uses code that looks vulnerable, but isn't, to check for false alarms.

Benchmark Project Vulnerability Categories

1. Command Injection
2. Cross Site Scripting
3. Insecure Cookie
4. LDAP Injection
5. Path Traversal
6. SQL Injection
7. Trust Boundary Violation
8. Weak Encryption Algorithm
9. Weak Hash Algorithm
10. Weak Random Number
11. XPath Injection

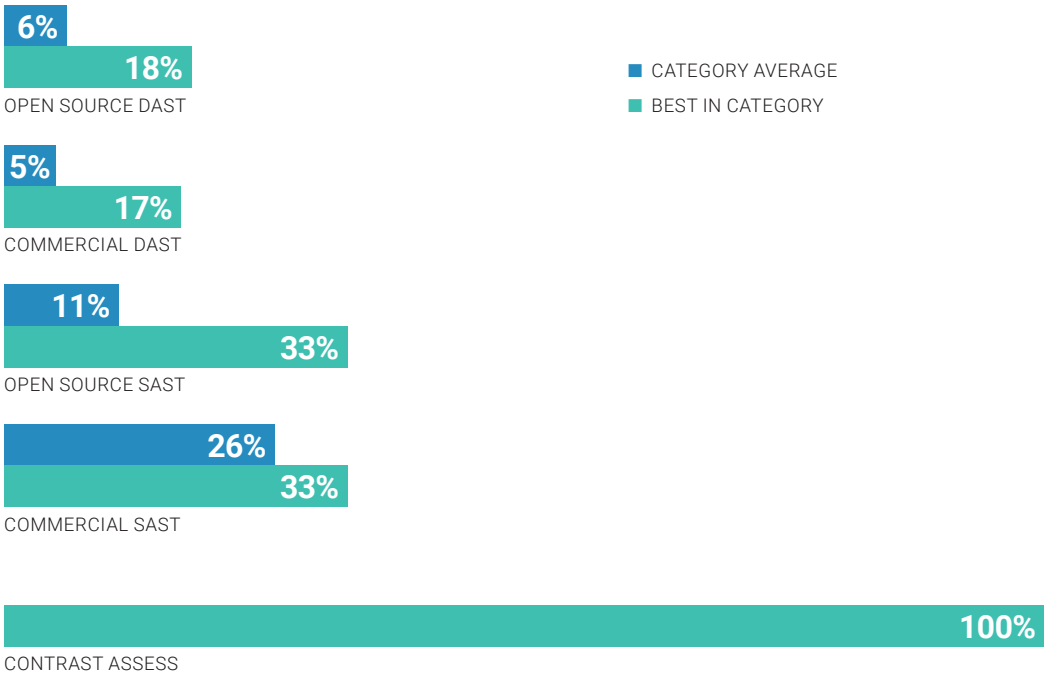
The Benchmark Project is rigorous, yet the application it provides for testing is still considerably simpler than typical corporate applications. So it serves as a good measure of accuracy, and as a litmus test as well: Any product that doesn't score highly on the OWASP Benchmark puts organizations at serious risk of missing major vulnerabilities in their real-world applications and generating lots of false alarms.

Applying the benchmark application consistently across application security testing products produced astonishing results on the accuracy front:

18%	Most accurate open source Dynamic Application Security Testing (DAST) product
17%	Most accurate commercial DAST product
33%	Most accurate open source Static Application Security Testing (SAST) product
33%	Most accurate commercial SAST product
100%	Contrast Enterprise, an Interactive Application Security Testing (IAST) product

Benchmark Accuracy Results

Accuracy scores for products across all 11 Benchmark Project vulnerability categories.



INCREASED ACCURACY AND SPEED DRIVE SCALE

The OWASP Benchmark Project also showed that commercial SAST and DAST solutions take a minimum of 3 hours (products) to two weeks (SaaS offerings) to complete their analyses. That's an unacceptable, disruptive delay for most organizations. The delay, combined with SAST and DAST inaccuracy, is why at most 10% of the applications in an enterprise portfolio get any security testing today. Contrast produced highly accurate results in about 5 minutes, which is transformational for enterprise application security initiatives. Organizations testing dozens or hundreds of applications can now scale their initiatives to secure hundreds or thousands of applications.

There is a Better Way

Businesses have been relying on SAST and DAST products for nearly 15 years to try to secure their applications and check off compliance requirements. Until recently, those products were a natural and rational choice. But, with the emergence of IAST solutions, and now with the OWASP Benchmark Project to quantify accuracy, it's clear there's a better way.

Reevaluate Application Security Products and Programs

Using the benchmark, organizations should evaluate the strengths and weaknesses of their current solutions, and reconsider their options. Contrast Enterprise, which the OWASP Benchmark demonstrated is both fast and accurate, is a natural choice to augment or replace existing SAST and DAST solutions. Ask your application security vendor for their benchmark results, and contact Contrast Security (benchmark@contrastsecurity.com) to learn more about Contrast Enterprise.

CONTRAST SECURITY

291 Lambert Ave
Palo Alto, CA 94306
888.371.1333

063017