SYNOPSYS®

# DAST TO THE FUTURE:

## Shifting the Modern Application Security Paradigm

## Where We Are: The Fallacy of Standalone Static Testing

The emphasis on securing applications in development has not resulted in the reduction of breaches that was once expected. In fact, breaches are becoming even more common and more dangerous.

In the weeks following the May 2021 ransomware attack on the Colonial Pipeline, the White House issued a sobering memo urging businesses to increase their cybersecurity efforts. The memo, published on June 3, 2021, notes that "the number and size of ransomware incidents have increased significantly, and strengthening our nation's resilience from cyberattacks—both private and public sector—is a top priority of the President's."

Here's the reality: testing applications solely in development cannot and will not protect them from being breached in production.

With static testing, developers secure what they "own" and move on. This is understandable; developers, after all, are largely focused on users, not security. Static application security testing (SAST) vendors know this. Forrester analyst Sandy Carielli recently noted in a blog post that "pretty much every vendor in the SAST market is thinking in terms of the developer."

But by doing so, they miss the opportunity to test for vulnerabilities that show up in an operational system. It doesn't matter if developers ship flawless proprietary code and apply the latest security patches to each open source component—which in 2020, netted-out to an average of 528 per application. Many vulnerabilities found in a production application do not exist in its source code and arise only when deployed into production.

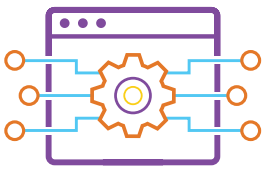
It's impossible to predict the universe of interactions between the millions of assets connected throughout the inherently dynamic application layer via APIs and integrations. That is the primary reason why the world's largest and smartest companies' applications are still getting breached.

If the ultimate goal of application security testing is centered around an idea of a digital future that is free from breaches, we must now embrace an approach to application security that is focused on accounting for the entire attack surface. And that means implementing continuous dynamic testing of web, mobile, and API applications, and integrating dynamic application security testing (DAST) insights to increase the efficacy of SAST and software composition analysis (SCA).

## Attack Surface Management: The Longstanding Thorn in AppSec's Side

Even in a prepandemic threat landscape, security teams continually struggled to accurately account for their organization's entire attack surface. Now, compiling a comprehensive inventory of the connected assets that make up an organization's attack surface can produce an overwhelming amount of information.

Speed, accuracy, and guidance are paramount in securing applications in production. Rather than having security teams sift through thousands of potential vulnerabilities, the first step in securing the application layer is to leverage an attack surface management tool that



Provides high-fidelity coverage of the attack surface

Uses artificial intelligence and machine learning to risk-rank vulnerabilities found in discovery

Offers human-verified guidance and actionable insights into DevOps (for remediation) and SecOps (for mitigation)

## APIs: The Application Layer's Wildcard

Not only are applications evolving at an increasing rate, but the digital threat landscape is also rapidly changing. The pandemic accelerated digital maturation across the globe, and alongside it, an explosion of API-first development that connects smart devices, personalizes users' online experiences, and allows businesses to integrate their tech stacks.

In 2022, Gartner expects that 90% of web-enabled applications will have more surface area for an attack in the form of exposed APIs rather than the UI, and API abuses will be the vector most responsible for data breaches. Gartner also projects that in 2022, APIs will become the most-frequent attack vector resulting in data breaches for enterprise applications.

APIs are a double-edged sword—they have proven to be critical in enabling developer teams to reduce the time it takes to build cloud-based applications and bring them to market, but when implemented poorly, they provide unprecedented access to core transactional business systems. For example, in May 2021, WhiteHat™ DAST data showed that at least 50% of applications in industries including manufacturing, public services, healthcare, retail, education, and utilities have at least one open serious, exploitable vulnerability.

Dynamic testing of APIs in production is more important than ever for identifying security vulnerabilities, but it's also vital for identifying business logic flaws that can result in unfettered access to user data by malicious actors across the digital supply chain.

Traditional business risks come from inheriting a partner; modern business risks come from inheriting a partner's applications.

## DAST-First: Testing Right to Shift Left

The way web, mobile, and API applications are built is continually changing, adapting, and progressing—they are, by definition, dynamic. Shouldn't the way we test them also be?

Implementing DAST is necessary to determine the security posture of applications running in production and how they will likely interact with end users. It has now also become essential for teams to keep up with the changing nature of applications and the knowledge of adversaries. Effective DevSecOps starts with taking feedback produced from DAST and integrating it into both SecOps and DevOps tools. After all, DAST finds the actual vulnerabilities that put an organization and its end users at risk.

It stands to reason that SAST without DAST will not decrease the likelihood of an application being breached. However, when SAST is implemented in addition to DAST, organizations can capitalize on benefits that cannot be achieved through one testing method alone. Fine-tuning SAST rules can prevent the volume of false positives found with DAST. Insights from DAST should guide teams to better configure their SAST parameters and influence more secure coding practices.

Unlocking the full potential of AppSec must include dynamic testing. But leveraging its insights to improve the efficacy of static testing and speed up the software development life cycle will help us reach the common goal of developers and security teams—happy, secure users.

## Driving the Future

The importance of a DAST-focused approach is analogous to building and testing a race car.

Race teams assemble their car using individual parts—pistons, the fuel injection system, tires, brake calipers, etc.—each of which (presumably) passed its manufacturer's quality assurance tests. With a solely static approach to testing, a team could assume that once assembled, the car will run at peak performance and keep pace with the field of competitors. There is no need for test laps because each component of the car will function as it should.

However, we know that is not the case—problems only begin to arise once rubber meets the road.

A DAST-focused approach recognizes that the thousands of individual components that make up the race car are now working together for the first time in an environment loaded with variables—the track, the weather, the skill of the team that assembled the car, the driver's experience, and more. Without dynamic testing—the test laps—the car is unlikely to perform up to its potential—not to mention the practice would be considered irresponsible and potentially dangerous.

Whether building a race car or a modern web application, teams that dismiss the critical importance of dynamic testing are likely to end up in the same place—at the back of the pack.

**Learn how the right DAST tool helps build security into your software—at the speed your business demands**

SYNOPSYS®

# The Synopsys difference

Synopsys Software Integrity Group provides integrated solutions that transform the way development teams build and deliver software, accelerating innovation while addressing business risk. Our industry-leading portfolio of software security products and services is the most comprehensive in the world and interoperates with third-party and open source tools, allowing organizations to leverage existing investments to build the security program that's best for them. Only Synopsys offers everything you need to build trust in your software.

For more information, go to www.synopsys.com/software.

**Synopsys, Inc.**
690 E Middlefield Road
Mountain View, CA 94043 USA

**Contact us:**
U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com