SYNOPSYS® Mi2 PARTNERING SUCCESS

CÔNG TY CỔ PHẦN TIN HỌC MI MI

Gartner® Magic Quadrant™ for Application Security

What capabilities are critical to the success of your AppSec program?

Source: www.synopsys.com

Aug 31, 2023 / 5 min read

By Patrick Carey

There are two cars in my driveway right now. One was built in 1978, and what's great about it is how easy it is to work on. It's a simple vehicle, and most repairs can be performed with only a half-dozen tools: two screwdrivers, three wrenches, and a hammer (you always need a hammer).

The other car was built in 2020, and I don't work on that one. It's vastly more sophisticated—and complicated—than the '78, and my mechanic wields a dizzying assortment of specialized tools and diagnostic systems to ensure that everything is working correctly.

And so it is with software. As the software we build has become more sophisticated—and complicated—the array of security tools required to test that software is expanding. In fact, most organizations today use dozens of tools and techniques to test their software for vulnerabilities.

But which ones should you be using? The answer to that question depends on the type of software you are developing and how you are delivering it.

Gartner recently published its 2023 Critical Capabilities™ for Application Security Testing report. It provides insight into which tools and techniques are most important for five specific use cases, as well as ratings and reviews of the vendors that provide those tools. Let's look at the five use cases in the report and the differences in their respective application security needs.

Download the report

Maximizing security for enterprise applications

Gartner defines the first use case as being focused on the needs of organizations with a broad mix of applications and development methodologies, and thus requiring a comprehensive approach to application security. Put another way, if your team builds software that isn't your product but is instead the primary enabler of your business (i.e., it is

the means by which your customers access your products or services), this use case applies to you even if you aren't a large organization.
The complex makeup and delivery of enterprise applications requires that security be addressed for all application components and at all stages of the application life cycle. However, many enterprises find that they are using and managing a dozen or more application security testing (AST) tools across multiple development teams. It can be difficult to "see the forest for the trees" when different teams use different tools that report security findings in different ways. Application security posture management (ASPM) solutions such as Software Risk Manager by Synopsys help enterprise AppSec teams bring order to the chaos. With ASPM, teams can define and automate uniform security policies across teams, and synthesize, filter, and prioritize findings across tools.
Learn more about Software Risk Manager

Securing the software supply chain

Organizations are increasingly taking a supply chain risk management approach to application security. In this approach, multiple tools are used in concert to provide visibility and control of security risks across proprietary, open source, and third-party software and services, as well as the DevOps pipelines and cloud infrastructure used to deliver applications to end users. This shift has been driven by high-profile software supply chain vulnerabilities and attacks, as well as by regulatory pressures from governments and agencies seeking to drive more secure software development practices by their vendors.

Software supply chain security is not separate from application security—it encompasses it. Organizations are realizing that it's not enough to simply to rough a prescribed set of security tests as part of their software development life cycle. They need visibility and control of their upstream software component suppliers and DevOps toolchain risks. And they likewise need to provide transparency into the makeup of their software for their customers in the form of Software Bills of Materials (SBOMs) and other artifacts. This end-to-end chain of visibility and control helps ensure that vendors and customers are armed with the information they need to proactively defend against cyberattacks targeting application vulnerabilities.

Learn how to secure your software supply chain

Building security into DevOps

DevSecOps is a term that means different things to different organizations. Gartner indicates simply that this use case is focused on the requirements of organizations investing heavily in DevOps and the fast-moving, iterative software development and delivery that goes with it.
Not surprisingly, for application security testing, the emphasis is also on tools that support modern, developer-centric, automated security analysis. Building security into DevOps requires that teams prioritize three things.

- Developer enablement: Providing developers with fast and efficient tools that help them address security defects while they are coding
- Intelligent AST orchestration: Optimizing automated security testing and ensuring that pipelines continue to operate at full speed
- Risk-based vulnerability correlation: Helping teams cut through the noise of their automated security test results to focus remediation efforts on what matters most to the business

Learn more about how to build security into your DevOps program

Securing applications in the cloud

There is considerable overlap between Gartner's prescriptions for cloud-native applications and DevSecOps. The main difference is that DevSecOps places a bit more emphasis on developer enablement, while cloud-native applications place a bit more emphasis on APIs, infrastructure-as-code (IaC), and the containers that are central to most cloud application environments.

Since many cloud-native applications are also enterprise applications, the focus on software supply chain security also applies here. However, it's important to understand the impacts of the cloud architecture on the attack surface of these applications, which typically use a mix of open source components, third-party APIs, serverless functions, containers, and IaC.

Learn more about Synopsys solutions for cloud and container security

Addressing the unique security needs of mobile and client applications

As the name implies, the fourth use case is focused on software that runs on client hardware. For Gartner, this means mobile applications, which often require specialized testing tools and techniques to emulate the target mobile device(s) for the application.

However, many of the challenges for mobile applications also extend to other forms of client-side software, such as network device firmware, embedded software, and IoT devices. In most cases, testing of this software is difficult to automate, requires direct access to or emulation of the hardware, and includes testing of the APIs or network protocols used for communication with other systems and services. If you are building this type of software, you probably already have specialized tools for unit and integration testing—the challenge is finding complementary tools and services to test for security defects.

Learn more about Synopsys application security testing tools and services

Building your AppSec program

There’s no doubt that it can be difficult for security and development teams to assemble the right toolkit to ensure that their users can trust that the software they deliver to them is secure. But as Gartner illustrates in the Critical Capabilities for Application Security Testing report, if you take a step back and think about the use cases your team is trying to support, a framework for making your tool selections emerges.
As for me, I’m going to stick to tinkering on the ’78 on the weekends and leave the diagnostics and service of the ‘20 to the shop where they have the right tools (and skills) for the job.