VERACODE Infosheet

Evaluating and Selecting AppSec Vendors to Fit Your Business Needs

Application security (AppSec) has seen quite an ***uptick*** over the last 10 years, with no signs of slowing down. When your organization is ready to tackle the challenge of building a strong AppSec program, you may find yourself wondering where to plug in various tools and solutions – and even where to start with comparing AppSec vendors.

How can you properly evaluate the marketplace and select the right solutions for your organization's needs? Consider a framework that combines developer enablement with AppSec governance for an approach that covers the needs of modern software development without breaking the bank. Here's a guide on what to look for when assessing potential vendors to determine whether they're the right fit for your business.

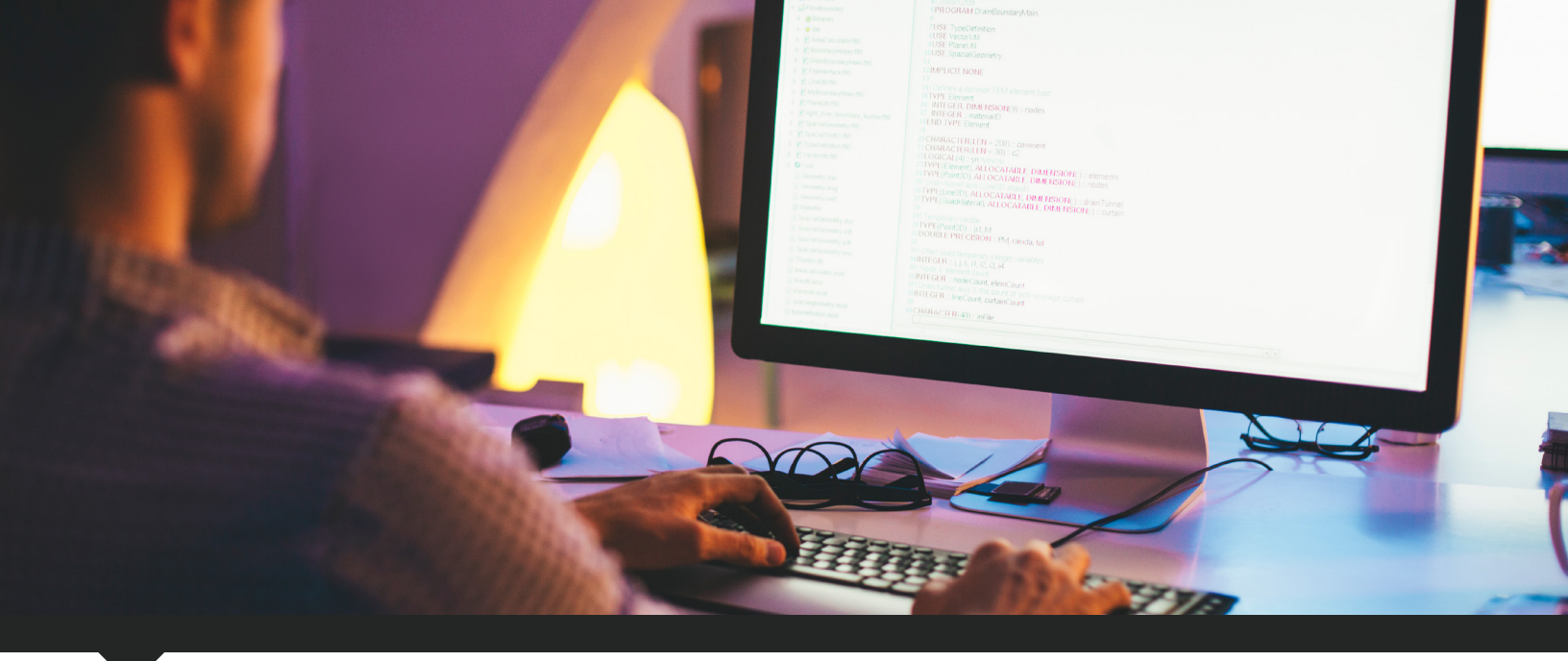
Range of scanning and testing technologies

Overcoming challenges in ***DevSecOps*** means the ability to scale up and scale down as needed. It also entails empowering developers to fix security issues on their own and easing efficiency with automated solutions.

As no one single tool can act as a window into the health of your AppSec, it's important to choose a vendor that offers several scanning and testing technologies with the ability to scale and automate from anywhere to bolster dispersed workforces. At the heart of developer enablement and AppSec should live comprehensive analysis tools with ***solutions*** like the following:

- **Static Analysis (SAST):** This test process is performed without executing the program, but rather by examining the source code, byte code or application binaries for signs of security vulnerabilities.
- **Software Composition Analysis (SCA):** This testing type identifies vulnerabilities in open source libraries that your team has included in the code.
- **Interactive Application Security Testing (IAST):** IAST uses an agent inside the application or runtime environment that observes where an application could be exploited when executed.
- **Dynamic Analysis (DAST):** Dynamic application security testing (DAST) looks at the application from the outside in — by examining it in its running state and trying to manipulate it in order to discover security vulnerabilities. The dynamic test simulates attacks against a web application and analyzes the application's reactions, determining whether it is vulnerable.
- **Penetration Testing:** A solution that goes beyond automated testing for a manual assessment of the health of your code

Note: Run an evaluation on the tools with your own applications, not standardized benchmark applications. Some vendors optimize results for benchmarking applications but deliver far worse results or require extensive tuning for custom apps. Insist that you will scan your own apps and want to be present for any tuning that needs to occur so that you can estimate the effort per application.



SaaS vs. on-prem solutions

When surveying options for vendors, it's important to decide whether ***cloud-based SaaS solutions or on-premises tools*** are the better fit. On-prem tools that require installation, setup time, training, and maintenance are typically not easy to scale and are more expensive, requiring a surplus of skills and time. That means organizations are slower to start scanning and securing their applications.

Cloud-based services, however, do not require businesses to buy tools and go through the process of installation and continued maintenance or patching. There is also less of a responsibility for the accuracy of detection as that falls on the vendor, and little to no downtime in running scans and receiving results that guide DevSecOps programs. When a vendor offers SaaS solutions in the cloud, they handle the deployment and upkeep swiftly so that organizations can start scanning from day one and don't have to worry about AppSec tools weighing on their processes (or servers) as they scale up and scale down.

AppSec governance solutions

Three of the key factors for ***AppSec governance*** include defining your program to achieve specific goals, scaling your program through best practices learned along the way, and proving the value of your AppSec solution. Good AppSec governance tools directly impact remediation management by informing decisions your security and development teams make, while also helping your organization meet compliance needs. Vendors that are thoughtful about AppSec governance offer solutions including:

- **Policy and Reporting:** Your AppSec vendor should have policy and reporting tools that provide a clear report on progress to help set goals, define SLAs, and meet compliance requirements.
- **Remediation Management:** Remediation management solutions enable your organization to fix found flaws quickly.
- **Analytics:** It's important for your AppSec vendor of choice to offer ***analytics tools*** that provide clear insight into metrics to help you manage and mature your DevSecOps programs, as well as demonstrate success.

Developer enablement resources

Developer enablement is critical to the success of your DevSecOps program, as developers are the ones creating secure code. Resources designed for enablement will help developers find and fix flaws faster, as well as reduce the introduction of new flaws. If your vendor of choice offers these resources to developers, you'll have an easier time opening a door of communication between development and security to ***shift AppSec left*** earlier in the development process. Focus on vendors that offer:

- **Integrations:** Ask potential vendors how they would handle integrations with your development pipeline, and what their range of compatible integrations looks like.
- **Training:** Vendors that offer developer training through real-time feedback while coding, workshops, and ***hands-on*** learning care about empowering your developers to write more secure code. Ask potential vendors what they offer for training materials, including programs that provide real-world experience breaking and fixing applications.
- **Remediation Guidance:** Remediation guidance is an essential part of developer enablement and ongoing training. Ask potential vendors what they offer for in-context guidance and one-on-one expert advice when it comes to your specific application types, and the programming languages your developers use most.

The numbers

Have a discussion with potential vendors about numbers that can shed light on their business wellbeing and, ultimately, the impact it will have on your organization's investment. To understand whether a potential vendor has the fortitude to meet your business needs, ask the following questions:

- How financially stable is this vendor?
- Will the vendor exist in the market in five to 10 years?
- What is the vendor's market share?

You can get a pulse on a potential vendor's standing in the market by looking at its:

- Revenue numbers
- Number of customers
- Number of scans completed
- Reputation among its audience
- History and track record of success
- Innovation and breadth of offerings

Finally, take a look at how much money potential vendors charge—and how much they'll cost you in the long run:

- What is the price per unit (tool, scan, etc.)?
- Carefully compare SaaS vs. on-prem solutions – the operational costs of on-prem solutions can be significant and should be scoped out before signing the paperwork.
- Can you consolidate various scan types into one vendor to reduce effort and get package deals?
- Does the solution require tuning of applications, maintenance, and operations? What is the labor cost associated with this?

Finding a vendor that fits the bill

Be prepared to approach each of your top options for vendors with questions about their suite of solutions and how they can fit into your existing processes. Look for vendors that offer multiple testing types like SAST, DAST, and SCA for a well-rounded approach to your application security.

Equally as important is finding a vendor with ***SaaS-based*** solutions in the cloud so that you won't have to delay projects or spend time waiting for maintenance down the road. If you can find all the above in a price range that fits your budget, you'll be well on your way to more secure applications that keep you - and your customers - safe.

Learn more about AppSec best practices, and how to get started, in our new guide, ***AppSec Best Practices vs. Practicality***.

VERACODE

Learn More

Veracode is the leading AppSec partner for creating secure software, reducing the risk of security breach and increasing security and development teams' productivity. As a result, companies using Veracode can move their business, and the world, forward. With its combination of automation, integrations, process, and speed, Veracode helps companies get accurate and reliable results to focus their efforts on fixing, not just finding, potential vulnerabilities.

Learn more at www.veracode.com, on the Veracode blog and on Twitter.