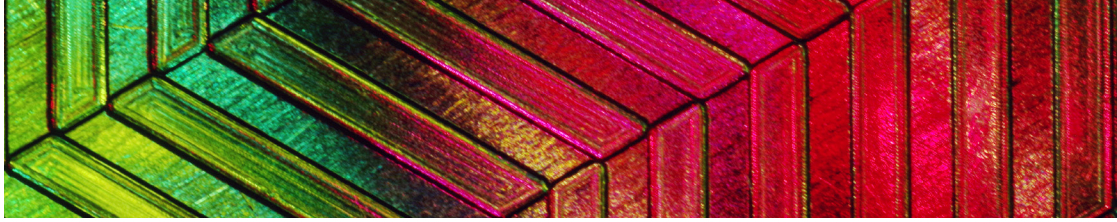
S&P Global
Market Intelligence
451 Research
Business Impact Brief



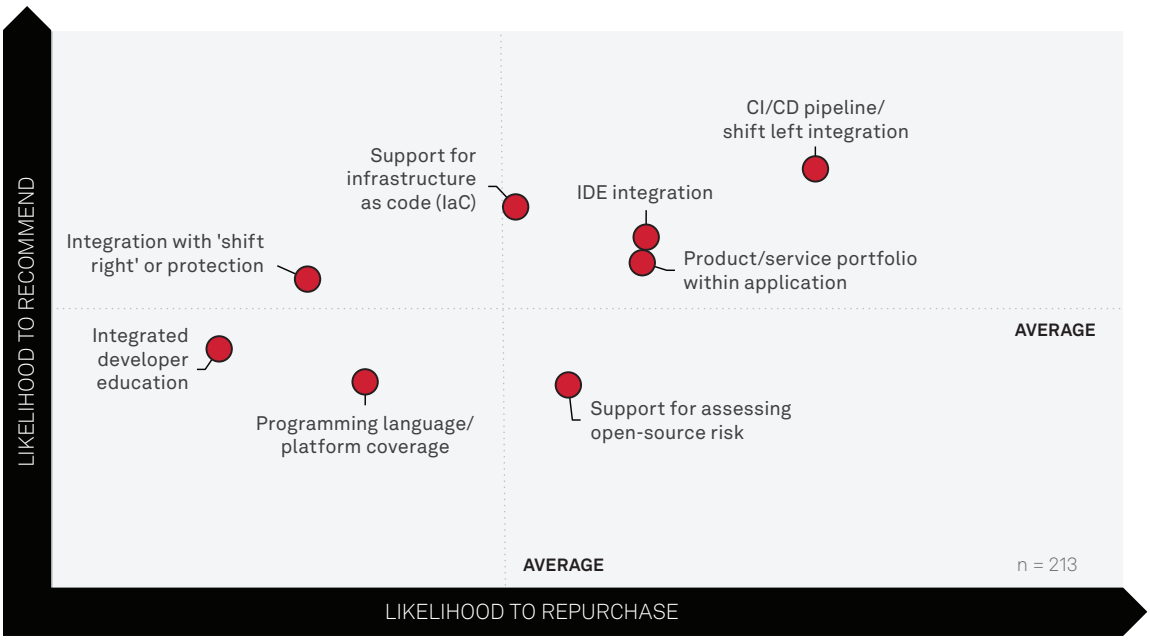
Shift right to shift left: Why an effective application security program looks both ways

The Take

Enterprise application security programs have spent years rightfully focused on "shifting left" — identifying and correcting vulnerabilities in applications and APIs earlier in the development process. The earlier in a development life cycle a problem is found and corrected, the less expensive and disruptive it will be to correct. Further, most organizations have more developers than security professionals capable of application security testing, so building security testing into application development provides a practical approach to maintaining a continuous security posture for applications.

In practice, "shifting left" is not so easy, and while it remains a goalpost, security concerns must take their place amid the various ways application developers are measured for performance, including timely delivery of features that advance business goals. Preproduction security tools and related processes that overtax developers and add excessive friction to writing and releasing code will result in developers seeking paths around the security team's guardrails, undermining the effectiveness of application security efforts.

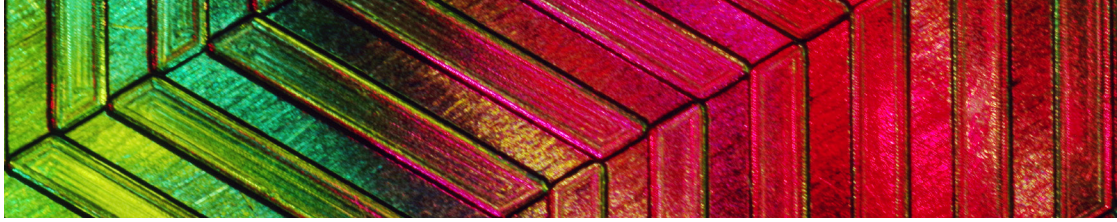
Correlation of factors influencing purchase of application security tools



We performed a correlation analysis between the vendor attribute ratings and likelihood to recommend and likelihood to repurchase.

Q. Thinking specifically about your primary application security provider, how likely are you to recommend them to a friend or colleague? Please use a 0-10 scale where 0 is "Not at all likely" and 10 is "Extremely likely." - Likelihood to recommend.
Q. How likely is your organization to purchase from your current primary application security provider in your next purchasing cycle? Please use a 0-10 scale where 0 is "Not at all likely" and 10 is "Extremely likely." - Likelihood to repurchase.
Q. How would you rate the level of importance of each of the following attributes when selecting an application security vendor?
Base: Respondents currently using application security or planning to over the next 12 months, abbreviated fielding.
Source: 451 Research's Voice of the Enterprise: Information Security, Application Security 2024.

Copyright © 2024 S&P Global. The content of this artifact is for educational purposes only. S&P Global Market Intelligence does not endorse any companies, technologies, products, services, or solutions. Permission to reprint or distribute any content from this artifact requires the prior written approval of S&P Global Market Intelligence.



Meanwhile, in the early stages of industry regulatory efforts such as PCI-DSS, "shift-right" solutions that protect applications in production were presented as an alternative to testing applications for security flaws. The false dichotomy that shift-right solutions eliminate the need for shift-left testing has eroded as the range of application protection solutions has evolved from early web application firewalls (WAFs) and runtime application self-protection solutions to runtime security, API security, the modern next-gen WAF, and application security posture management. Rather than a choice between AST and application protection, a combination of the two gives enterprises a fighting chance against today's application security threats.

The chart above examines features of preproduction security solutions that are most likely to motivate repurchase or recommendation to industry colleagues. These include table-stakes features such as coverage of programming languages and detection of open-source risks, as well as differentiators such as the ease of CI/CD integration. According to these results, one of the key factors influencing the likelihood of recommendation is integration with shift-right technologies. This interplay between toolsets is important for several reasons.

Business impact

Live production context provides for real prioritization. Common vulnerabilities and exposures and related vulnerability scoring can provide a broad sense of the potential impact of a known vulnerability. However, these resources cannot address an enterprise application's specific operating context, such as what vulnerabilities attackers are attempting to exploit and which vulnerabilities are part of code that is internet-reachable. When developers are overwhelmed by scanning tool results, issue prioritization based on real-world context for specific applications can be a filter to help focus remediation efforts.

Blocking attacks in production creates space for developers and security teams to work. Identifying a serious vulnerability is only one step in a remediation process that includes designing, applying and testing a fix. Urgency increases when the discovered vulnerability is being exploited by attackers in production, and yet security teams often cannot dictate that "nobody goes home until this is fixed." Security tooling that blocks attacks that leverage a common vulnerability (sometimes referred to as a "virtual patch") creates space for developers and security teams to work through and test corrective action. The right blocking solutions also borrow from DevOps principles by allowing for testing — for example, a new WAF rule — prior to deployment.

Not every problem is a known problem created by new development — newly discovered zero-day attacks are also a consideration. When a newly discovered open-source vulnerability in a widely used library is disclosed, such as the Log4J vulnerability, the first step is to determine everywhere that library is used. Next, the fix must be applied, usually in the form of a corrected version of the affected library, which includes testing to determine whether applications will work with the new version. Such high-priority vulnerability remediations do not benefit from a panicked rush. Shift-right protections allow for the blocking of new and novel attacks, providing space for developers to implement corrective measures.

Looking ahead

Two things are clear. First, the view that shift-left and shift-right approaches compete or are mutually exclusive has eroded. Today's application security practitioner views integration with shift-left application scanning as a key competitive aspect of shift-right tools and a key reason they would recommend a particular vendor solution.

Second, shift-right or application protection solutions have become more varied and sophisticated. Interplay with code scanning results, software composition analysis or dynamic/interactive application security testing has become a practical reality and a functionality that buyers expect. Application protection solutions such as a next-generation WAF can leverage threat intelligence — collective intelligence anonymously gathered from other WAF customers — and develop blocking rules to defend against new and novel attacks. API security solutions can identify which APIs contain sensitive data and are under attack, and like WAFs, can share data on production attacks with time-constrained developers prioritizing what to fix and in what order.

While reciprocal sharing of intelligence between AST scanners and production application protection tools is emerging as a practical reality, it is still in early stages. The chart above references "integration," and that concept remains the key to effectively leveraging information across the complex and often fragmented enterprise application security tool estate. The first step toward greater integration is viewing shift-left and shift-right tools as complementary and equally critical to an effective application security strategy.

fastly®

As you shift right to shift left, your organization inches closer to a DevOps (and even DevSecOps) culture that enables collaboration between development and operations teams throughout the entire software delivery lifecycle. This results in robust processes, exponential improvements in deployment times, and, ultimately, superior results for a company's bottom line. Check out Fastly's DevOps Roadmap for Security to learn about the four transformational areas of DevOps and how a better WAF can help you shift-left more effectively.