5 Ways to Boost AppSec Performance and Returns

Key Takeaways From the Joint Veracode and ESG *Application Security for Contemporary Software Development and Deployment* **Survey Report**

There's growing recognition that software development efforts must be tightly linked to application security. Yet as organizations attempt to navigate an increasingly complex IT environment — one that incorporates DevOps and other agile practices — requirements are constantly shifting. As a result, many organizations struggle to keep applications protected and coding practices secure and up-to-date.

A recent Veracode and ESG report, *Application Security for Contemporary Software Development and Deployment*, looked at the survey responses of 400 IT, cybersecurity and application development professionals. Researchers found that business and IT executives are increasingly aware of the need for integrated security and are putting greater resources into addressing application security and DevOps, and even moving toward DevSecOps. These organizations are realizing benefits from this emphasis of linking coding practices and cybersecurity.

But challenges remain. Here are five key findings from the report that reveal the issues that IT professionals must address:

1

Educating and enabling developers is crucial.

One-third of those surveyed by ESG indicated that the functionality of their code is their single most important metric. Unfortunately, many developers view security as an obstacle. In fact, ESG found that 22 percent of respondents believe that security interferes with their ability to code so they avoid the security team.

The study also found that organizations are recognizing the need for training and more advanced tools. One-third of survey respondents indicated that all developers at their firms are required to perform static application security testing (SAST) as part of unit testing before code is checked in, while 31 percent will incorporate dynamic application security testing (DAST) into their automated test and production environments through integration with DevOps tools.

2

DevOps enables application security.

About half (45 percent) of IT professionals believe that DevOps has made their job easier by streamlining integration, testing and delivery. Furthermore, 43 percent said that correcting security defects in the development stage is more efficient than patching production systems. As the use of Agile and DevOps accelerates — just 5 percent of organizations reported not using these methodologies — there's a growing recognition that agility and security are deeply intertwined. DevOps is perceived as having a net-positive effect in streamlining the development process and enabling the integration of security testing, the report states.

3

Automation is key to better security.

An acute shortage of cybersecurity professionals and a lack of skills among those in the field have forced organizations to become more operationally efficient. At the center of the equation is automation. "Application developers and security teams have reaped security benefits from DevOps, easing automation of security testing," ESG notes. Only 8 percent said that injecting application security into DevOps has slowed production. Another way organizations are putting automation to work is through routine validation of software composition to "understand the provenance of components." Just over two-thirds of organizations rely on this approach.

4

Mobile-first and cloud-first equalize AppSec priorities.

Mobile and cloud have emerged at the center of software development. In fact, many organizations must prioritize development in these two areas. But optimizing applications to run on mobile devices before working on versions for the desktop and in the cloud introduces new requirements for application security. "When deploying new or existing applications, organizations should consider and fully evaluate potential cloud solutions first before considering on-premises or legacy infrastructures," ESG states.

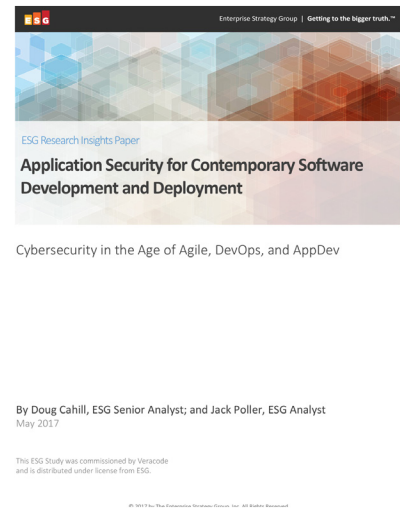
With traditional application development distinguishing between internal and external apps, the study found that there's a perception that internal apps are safer than external apps. In addition, traditionally, internal apps were tested statically, while external apps were tested dynamically. But as lines blur about what's internal and what's external, there's a need to focus more on static and dynamic testing of all apps. Simply put: AppSec and AppDev should become a best-practice approach, regardless of the app or usage model.

5

Make application security a priority across the enterprise.

The study found that 58 percent of respondents focus on a team approach when it comes to security and development. Within these organizations, application development and security teams work collaboratively to prioritize which security-related defects are addressed based on their severity, as well as on the likelihood they will be exploited. ESG recommends that organizations make security a primary metric for all owners, from development to testing to production. Moreover, product owners should create and relate AppSec stories as part of the Agile sprint and scrum.

As application architectures evolve and organizations undergo digital transformation — including mobile, cloud and IoT-first initiatives — the need for a more cohesive and automated approach is paramount. As ESG emphasizes, security cannot take a back seat to functionality.



For more details on the ESG report, *Application Security for Contemporary Software Development and Deployment*, visit https://info.veracode.com/analyst-report-veracode-appsec-and-devops-trends-esg-survey.html

VERACODE