Introduction

Integrating application security (AppSec)—the technologies used to detect and address potential security issues in software—into your software development life cycle (SDLC) and your DevOps pipeline is increasingly important in a development environment characterized by continuous integration/continuous development (CI/CD) workflows. AppSec integration allows security teams to establish security gates at multiple stages of the development and deployment process, which helps you avoid late-stage testing and the development rework that ensues. Late-stage testing and development can delay releases or lead to overlooked risks being promoted into production. This approach is commonly referred to as "shifting left" in the development cycle or, increasingly, as "shifting everywhere."

True AppSec integration requires combining and connecting elements, systems, and processes to work together seamlessly. It involves merging disparate components into a unified system, enabling the smooth flow of information, functionalities, or resources. Moreover, integration means these elements and systems fit naturally into established workflows—preventing teams from architecting new workflows that disrupt teams and diminish efficiency.

In the context of software development and application security, integration plays a crucial role in achieving important business objectives, including

- Mitigating risks that could threaten sensitive data
- Supporting compliance initiatives for security practices
- Elevating efficiency standards during development, testing, and deployment

AppSec integration extracts information and delivers risk insight

AppSec integrations make it possible to extract valuable information from various stages in the pipeline and enable you to deliver risk insight directly into developer workflows at the point where they can mitigate those risks as they continue their development work. This helps organizations establish automated processes that accelerate risk detection and prioritization, and prevent issues from proliferating downstream—all without risking missing a software shipping deadline.

AppSec integrations capture and extract data from multiple sources including development tools, code and binary repositories, version control systems, build systems, testing environments, and production environments. These integrations also allow organizations to run the right tests, at the right time, and at the right depth. This means security teams are not constrained to a single tool or testing protocol at a time. Rather, relevant tests run at various stages of the DevOps pipeline mitigate pipeline congestion.

Additionally, such integrations help teams catch vulnerabilities that may have been introduced at any stage of the development process, such as a developer checking a third-party binary or component into a repository without performing early-stage testing. Using integrations enables you to add a level of redundancy into your security testing at each stage, which helps ensure that nothing is missed.

AppSec integration also allows organizations to deliver risk insights at multiple points across the pipeline. This type of integration means security-related data such as code scan results, security event logs, and vulnerability alerts is disseminated efficiently and aligned to organizational standards for risk tolerance. Getting this information into the hands of those who can use it to fix associated security issues enables organizations to propagate informed decisions about risk prioritization and mitigation strategies, without being limited by subjective assessments of risk or inadequate security capabilities among developers and DevOps teams.

These two concepts—assessing risk and delivering actionable risk intelligence across the SDLC and DevOps pipelines—are fundamental to elevating AppSec programs to achieve DevSecOps. As software development and deployment become more interconnected, AppSec testing must become an intrinsic part of this framework rather than an appendage.

Security as a business driver

Security is essential to any business because, at the very least, it keeps you from running afoul of regulatory guidelines or
er mf ol.8 st f ºcd pr u8-5e nsmissof . prf r.8a lYSecur.4ui.29korr38ore.Durchase.520.orfirst astcf 8ct -3.e1.15prf r.3 53.a lyore.Durganiza of ,2[c

Synopsys provides integrated solutions that transform the way you build and deliver software, accelerating innovation while addressing business risk. With Synopsys, your developers can secure code as fast as they write it. Your development and DevSecOps teams can automate testing within development pipelines without compromising velocity. And your security teams can proactively manage risk and focus remediation efforts on what matters most to your organization. Our unmatched expertise helps you plan and execute any security initiative. Only Synopsys offers everything you need to build trust in your software.

For more information, go to www.synopsys.com/software.SynBT/CS0 cs/GS1gw /