BLACKDUCK®

Scaling DevSecOps: Continuous Testing That Evolves with Your Business

Overview

Companies that develop software today do so with teams dispersed around the globe, and that requires multiple development pipelines to accommodate a variety of software and development protocols. This means relying on cloud-based development resources to build many different software types, including containerized architectures, open source code, proprietary code, third-party binaries, and commercial software.

As the digital landscape evolves, so too do the challenges of securing this ever-changing environment. With the rise of new projects, team expansions, mergers, acquisitions, and the rapid adoption of new technologies like AI, organizations cannot afford to constantly redesign their DevSecOps programs.

We all know that continuous testing is a crucial aspect of a robust DevSecOps program. So it's vital to adopt a flexible and scalable testing approach that can adapt to these dynamic changes without requiring frequent overhauls.

Building Security Without Impeding Velocity

The first step to establishing an enduring DevSecOps initiative is to ensure that it won't slow down your development teams' velocity. As organizations have evolved from a "shift left" mindset to "shift everywhere," security testing has moved from the end of the development cycle back into the SDLC. This means that your teams are testing and remediating as part of their code, build, and ship workflows.

This requires organizations to rein in development tool proliferation, enact systems to prioritize results, and implement continuous testing and closed feedback loops between development and security teams.

Business and technology changes are ubiquitous, so you need an approach that not only protects the systems you're working with now, but that can scale and adapt as your business changes. When AppSec and DevOps teams have to redesign DevSecOps programs with each pipeline modification, your business velocity is going to get bogged down. So how do you address the problems of velocity and scale?

Building Collaboration with a Scalable Security Testing Platform

Given these challenges, a hosted, software-as-a-service (SaaS) security testing platform emerges as the optimal solution. A solution that integrates static application security testing (SAST), software composition analysis (SCA), and dynamic application security testing (DAST) engines will cover the multiple technologies being used across your organization, while enabling application security and development teams to collaborate in real time and meet release deadlines.

This approach offers several key advantages.

- A hosted, SaaS testing platform can easily scale to meet the growing and evolving needs of your organization while minimizing the administration and management burden of implementing various testing tools.
- It's flexible and supports a wide range of tests to ensure comprehensive security coverage.
- It integrates across various environments, pipelines, and tools, allowing teams to embed security tests across the SDLC and CI pipelines while managing one set of integrations, plugins, and templates.

- Centralized administrative controls allow security policies to be applied consistently across all projects, pipelines, and clouds.
- A unified dashboard provides a clear view of your security posture across all your business units, projects, and teams.

When your teams can identify and fix vulnerabilities as early and quickly as possible, with tools that deliver clear risk insight right to the developer desktop, you can ensure comprehensive compliance, regardless of whether your code is developed in-house or built using open source, third-party, or AI-generated code.

Building Flexibility into DevSecOps

Establishing a robust DevSecOps initiative in a large organization where work is shared among various teams and stakeholders is challenging, and redesigning security programs every time the technology or organization changes is impractical. To ensure that your security programs are consistent and resilient, you need to plan for the evolution of your development pipelines, your security requirements, your risk tolerance thresholds, and the software you're putting into the world.

There are three key areas where you need flexibility in your DevSecOps program.

- You need a program that can flexibly run the right tests at the right time so that your developers are remediating issues before they get into production. You want the kind of program that can, for example, scan artifacts as they get checked into source code management (SCM) repositories to see if anything new has been introduced, notify developers of an issue that needs to be fixed, and provide remediation guidance.
- You want a program that allows your teams to use their standard workflows. Development teams work most efficiently when they can customize their tools and workflows, so the system should allow them to use their preferred plugins for DevOps tools, automatically open fix pull requests when there are policy violations, and integrate with issue management systems.
- You want a program with testing engines that support a wide range of languages, frameworks, and architectures. Not only does this make it seamless to integrate with your existing AppSec program, but it future-proofs your organization by allowing developers to innovate and use new tools and workflows.

How Black Duck Can Help

The Black Duck® Polaris® Platform is the flexible and scalable platform you need. It is designed to evolve with your business and adapt to secure development pipelines. And it supports your entire integrated DevSecOps program with

- A cloud-based, SaaS architecture to simplify administration and management of mission-critical security tools
- Powerful security testing engines, including SAST to analyze proprietary code, SCA to analyze open source and third-party libraries, and DAST to analyze applications at production runtime without slowing down performance
- Centralized controls so you can easily ensure full security coverage across pipelines, teams, and business units
- A single source of truth about your security risk posture and priorities, where results from all your tests are consolidated and correlated against your standards and compliance needs
- Automated, bulk SCM onboarding that automatically detects new projects and branches in SCM repositories, ensuring that all new work and changes are added to test queues and continuously monitored
- Centralized policies that define risk tolerance and establish integrated security gates across your SDLC and CI pipelines
- Workflow integrations that send clear guidance to developers about where an issue exists, which contributing events invoke exploitable conditions, and recommended patches or modular secure coding training about how to fix that issue

Black Duck also offers a range of extensions and plugins to empower your developers to code securely in real time, and ensure the flexibility of your pipelines going forward.

- Code Sight™ IDE plugin allows developers to run local tests quickly and view results from pipeline-based scans conducted with Coverity® Static Analysis, Black Duck, or Polaris.
- The Black Duck GitHub Action, GitLab Template, Azure DevOps Extension, and Jenkins Plugin enable seamless connectivity to test servers, allowing developers and DevOps teams to embed security testing into their standard workflows. Once configured, security checks run automatically, enforcing policies and risk tolerance without requiring additional setup from developers.

In addition, Polaris helps you build security-aware and security-capable development teams. Developers are fundamental to your business, and by equipping them with the tools and knowledge to write secure code, organizations can introduce fewer vulnerabilities, reduce the workload on security teams, and expedite the resolution of identified issues. The Polaris platform's adaptability ensures that your security practices remain consistent, even as your organization grows and changes.

All of which means your business is set up for success now and in the future.

Learn more about the Polaris

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.