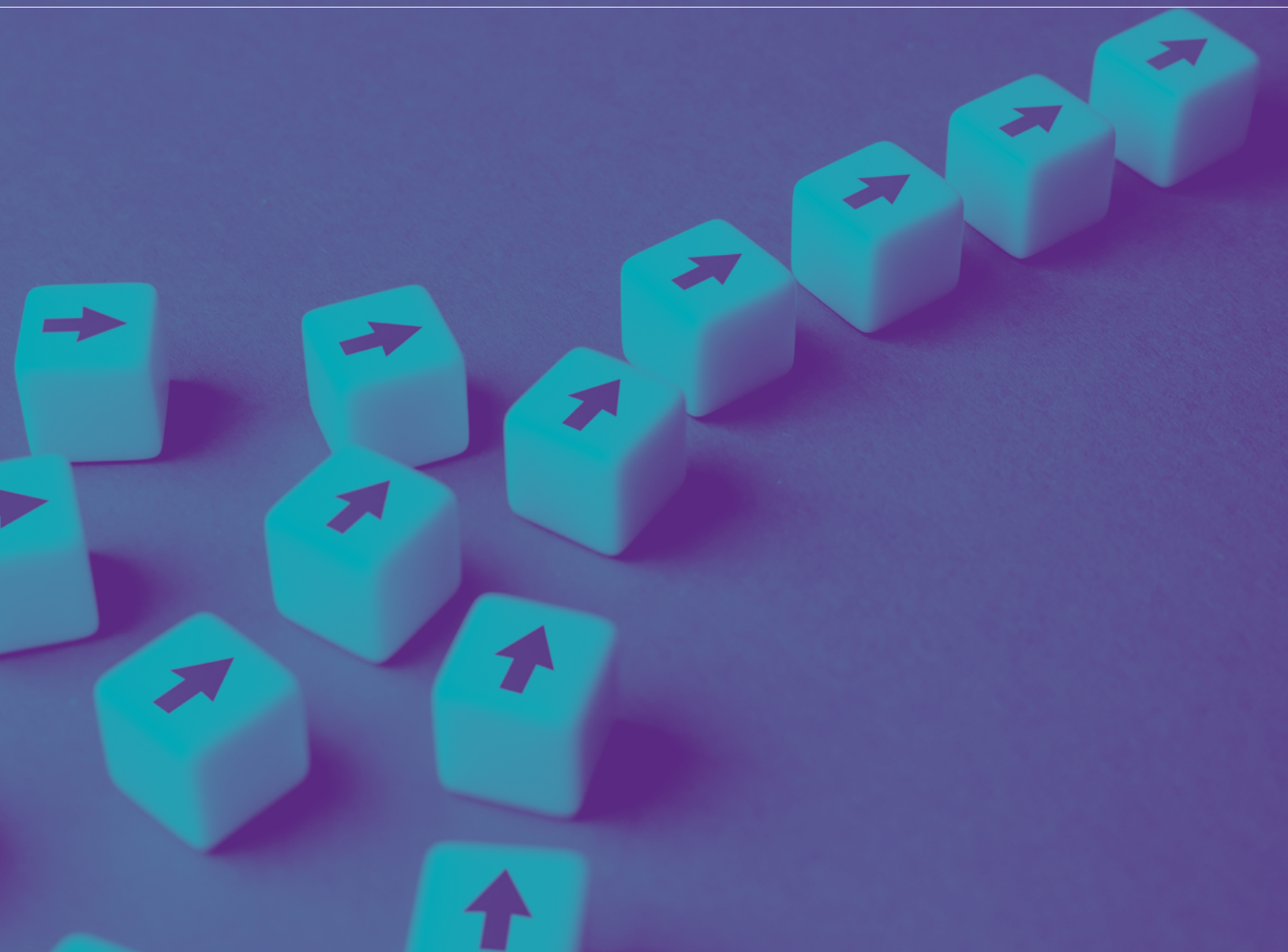
BLACK DUCK®

SIMPLIFY APPSEC
RISK MANAGEMENT

MAKE APPLICATION SECURITY TESTING FRICTIONLESS, AUTOMATED, AND EASY



Application security testing (AST) has become a mainstream component of software development in nearly every industry. But testing across applications, projects, branches, and test types inevitably produces myriad findings that lack context, alignment, prioritization, and other necessities for timely remediation. This complexity makes it difficult to manage overall application security risk.

Organizations need a solution that simplifies onboarding, integration, and automation of security tests within the integrated development environment (IDE), source code management (SCM) repositories, continuous integration (CI) tools, and other DevOps processes. And it needs to do that without compromising the type or level of scanning needed—all while making it easy to measure and track progress.

This guide shows security decision-makers how to simplify their application security approach so that development teams don't get bogged down and risk posture isn't compromised.

AUTOMATE THE ONBOARDING OF NEW PROJECTS

With thousands of apps to manage, the average enterprise can't afford the time and effort of onboarding them to individual AST tools. Onboarding inefficiencies reduce security accountability from the outset and make it difficult to centrally track code changes, testing status, or new updates across applications.

Automated bulk onboarding greatly reduces the time and effort required to monitor critical events and determine necessary checks. It also significantly streamlines the security testing process, enabling faster vulnerability detection, consistent application evaluation, and early intervention. This reduces the risk of security issues slipping through the cracks due to manual delays or oversight, ultimately improving overall application security and compliance.

Organizations need an AST platform that offers automated discovery along with bulk and continuous onboarding of applications and projects across disparate SCM repos, and it should be able to upload files by simply pointing to any repo. Additionally, automatic SCM event tracking and project syncing ensure that projects and branches in the AST platform are updated automatically without any intervention by developers.

INTEGRATE AST WITH EXISTING DEVOPS TOOLS

In addition to onboarding new projects automatically from SCM repos, it's important to integrate security tools directly into the developer's CI/CD tools and remediation workflows.

Complex security tools that disrupt developer workflows while adding the responsibility of incorporating security checks into their code without clear guidance is a recipe for failure. Such inefficiencies delay release deadlines and can cause developers to forego necessary security tests and/or fixes to problems. This explains how nearly one-quarter of all software releases include at least one security vulnerability.

To enable rapid development while maintaining robust security standards, organizations should seek a platform that provides

- **Extensive automation** throughout the software development life cycle (SDLC)
- **Security checks** throughout the SDLC ("shift everywhere")
- **Security feedback** delivered to developers directly via issue trackers and IDEs
- **Continuous monitoring** of events
- **Quick adaptation** to changing security threats and compliance requirements

AUTOMATE ANY SCAN, ANYTIME, ANYWHERE—ALL AT ONCE

Large applications running on modern architectures with complicated configurations, and often with constrained resources, require security scans that are simplified through automation and issue prioritization at scale. Otherwise, organizations are setting up their development teams for long testing and triage cycles to find the few critical vulnerabilities that matter to them.

Long scan times can hold up release cycles, especially when they're integrated into CI/CD pipelines, as developers need to wait for scan results before proceeding to deployment. This can lead to delays in product releases and updates, creating critical competitive disadvantages when it comes to customer delivery.

Instead, security teams should utilize custom scanning, whether rapid or full-scan analysis, tailored to the risk profile of the application or business. This ensures that the organization is checking for only the vulnerabilities relevant to its technologies and environment. The right AST platform can ensure this custom scanning for all scan types—static, dynamic, and software composition analysis—concurrently, across applications and projects, without adding any friction to pipelines and workflows.

Long scan times can hold up release cycles, especially when they're integrated into CI/CD pipelines, as developers need to wait for scan results before proceeding to deployment.

POLARIS PLATFORM

Black Duck Polaris™ Platform is an integrated, cloud-based application security testing solution optimized for the needs of development and DevSecOps teams. Polaris brings market-leading security analysis engines together in a unified platform, offering comprehensive intelligent risk management with the flexibility to run different tests at different times based on the application, project, schedule, or SDLC events. Our best-of-breed testing means developers don't have to slow down to cope with false positives, lack of scale across their projects and applications, or other issues that create friction in their workflows.

Polaris enables your organization to automate scanning and policy enforcement with the development and DevOps tools you're using today. It connects easily and directly to SCM repos such as GitHub, GitLab, Bitbucket, and Azure, with the ability to set schedules for automated scanning of projects.

By connecting Polaris to Jenkins and other CI tools, you can trigger scans with the option to break the build or send email alerts based on policy violations. And Polaris offers triage and prioritization management within its UI, plus the ability to assign them directly to developers via Jira and other issue trackers.

Polaris allows you to triage vulnerabilities, simplify analysis, track progress, and analyze trends all in one unified dashboard.

Learn more about how Polaris can help your organization simplify application security risk management

ABOUT BLACK DUCK

Black Duck® meets the board-level risks of modern software with True Scale Application Security, ensuring uncompromised trust in software for the regulated, AI-powered world. Only Black Duck solutions free organizations from tradeoffs between speed, accuracy, and compliance at scale while eliminating security, regulatory, and licensing risks. Whether in the cloud or on premises, Black Duck is the only choice for securing mission-critical software everywhere code happens. With Black Duck, security leaders can make smarter decisions and unleash business innovation with confidence. Learn more at www.blackduck.com.