

BLACK DUCK POLARIS PLATFORM

ONE PLATFORM, COMPLETE APPLICATION SECURITY

The no-compromise AppSec platform built for the speed, scale, and ambition of AI-powered development.

OVERVIEW

Black Duck Polaris™ Platform is a cloud-based application security platform optimized for modern DevSecOps. It integrates seamlessly into development workflows, prioritizes risks, and ensures policy adherence without compromising speed or accuracy.

KEY BENEFITS

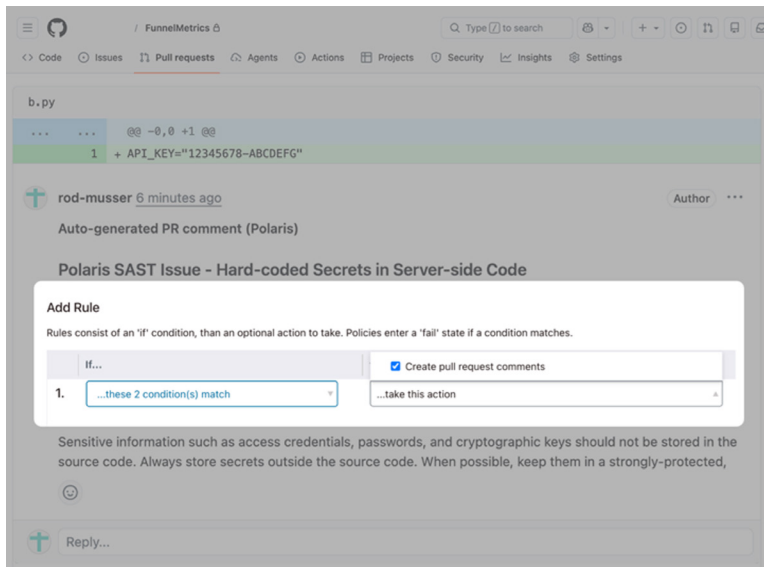
- **Developer-first workflow and integrations.** Security seamlessly integrated into development workflows for zero friction and maximum efficiency.
- **Risk prioritization and noise reduction.** Focus on the 5% of issues that drive 95% of risk, eliminating false positives and low-priority noise.
- **Policy, governance, and compliance.** Centralized governance with customizable policies to enforce security standards across the full SDLC.
- **AI-driven security and automation.** AI-powered remediation guidance provides real-time issue summaries and one-click fix suggestions.
- **Comprehensive scanning with depth and accuracy.** Market-leading SAST, SCA, and DAST engines deliver unified, accurate, and comprehensive results.
- **Visibility that proves ROI and risk posture.** Interactive dashboards and reports provide real-time insights into vulnerabilities and security program value.

“Black Duck’s ability to align to security-defined policies while functioning on automated pipeline triggers—things like code commits, pull requests, and builds—means that scans can run as early as possible while accommodating project nuances, contextual changes, and risk tolerance.”

—Michael Knight, VP of Technology at Datascan

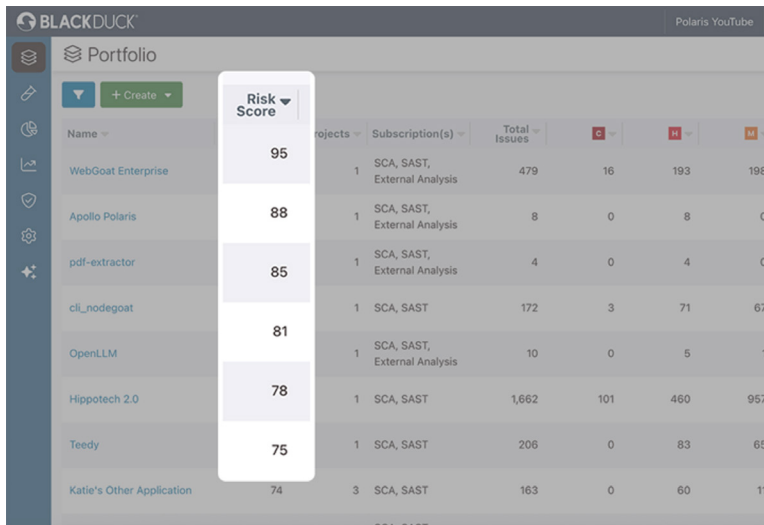
FEATURES THAT DRIVE SECURITY WITHOUT COMPROMISING SPEED

Developer-First Workflows



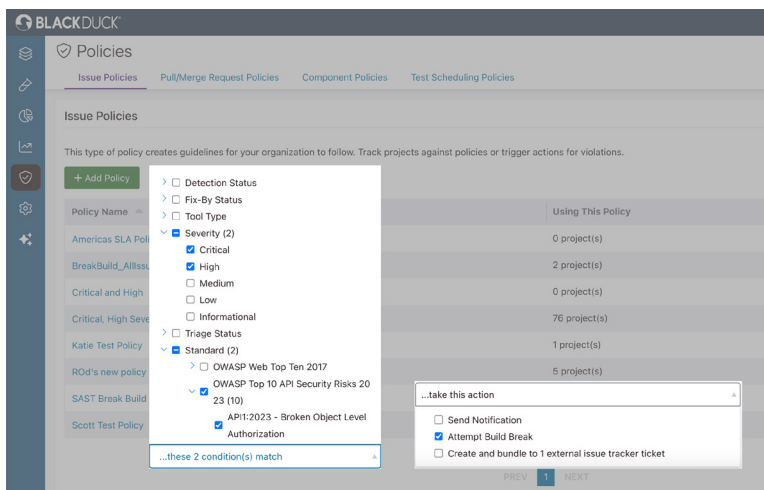
- Run automatic bulk SCM onboarding and discovery of new repositories for instant scanning and AppSec risk profiling.
- Reduce downstream risk by running rapid scans on pull requests with results posting as PR comments for fast, in-SCM feedback.
- Trigger full scans on code merges with findings flowing into Jira or ADO instances.

Risk Prioritization and Noise Reduction



- Let developers fix what matters and move on with consolidated SAST, SCA, and DAST results with intelligent scoring.
- Get an integrated risk score that includes environmental, business, and application risk profiles.
- Identify vulnerabilities and prioritize them based on severity, risk score, alignment with standard violations, and reachability.

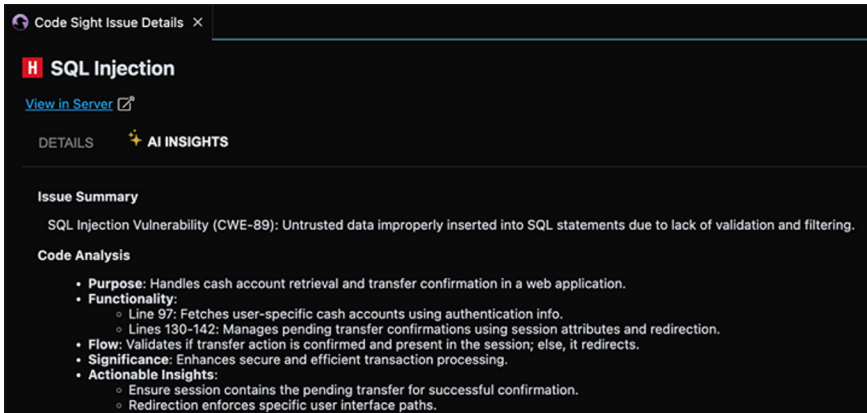
Policy, Governance, and Compliance



- Ensure centralized governance with customizable policies tailored to business risk profiles.
- Automatically enforce security standards across the SDLC by breaking the build, blocking pull requests, and sending notifications when a policy is in violation.
- Track which teams meet security targets and prove adherence to policy through reporting and tailored dashboards.

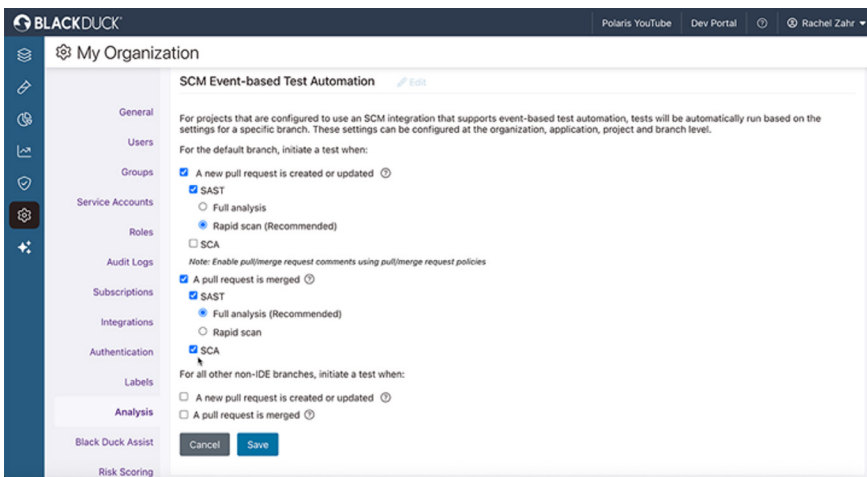
AI-DRIVEN SECURITY, COMPREHENSIVE SCANNING, AND PROVEN ROI

AI-Driven Security and Automation



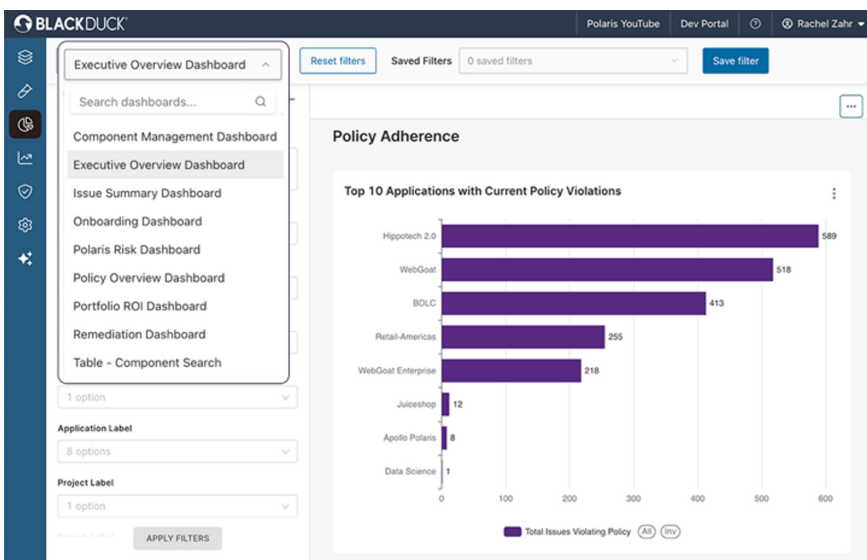
- Get one-click, quality fix recommendations directly in IDEs and pipelines with Black Duck Assist™.
- Help your developers learn secure coding patterns as they work through contextual security training that automatically provides context to findings.

Depth, Accuracy, and Comprehensiveness of Scanning



- Get market-leading SAST, SCA, and DAST engines integrated into one platform.
- Receive instant feedback by triggering a rapid scan or initiate a full scan for deeper more comprehensive analysis.
- Ensure broad coverage for popular languages, frameworks, and package managers, as well as IaC, API, and secrets scanning.

Visibility That Proves ROI and Risk Posture



- Get a real-time, unified view of application risk through interactive dashboards.
- View built-in reports for C-suite metrics, such as vulnerability burndown rates and policy compliance.
- Gain insights to prioritize resources and demonstrate security program value.

LANGUAGE AND PACKAGE MANAGER SUPPORT

SAST languages

- SAST languages
- Salesforce Apex
- C/C++
- C#
- DART
- Go
- Java
- JavaScript
- Kotlin
- Objective-C/C++
- PHP
- Python
- Ruby
- Scala
- Swift
- TypeScript
- Visual Basic

SCA package managers

- Apache Ivy
- BitBake
- Cargo
- Carthage
- CocoaPods
- Conan
- Conda
- CPAN
- CRAN
- Dart
- Erlang/Hex/Rebar
- Git
- Go Dep
- Gogradle
- Go Modules
- Go Vendor
- Gradle
- Hex
- Lerna
- Maven
- Npm
- NuGet
- Packagist
- PEAR
- Pip
- Pnpm
- Poetry
- RubyGems
- SBT
- Swift and Xcode
- Yarn

IAC, CLOUD, CONTAINER, AND CONFIGURATION FORMATS

- Ansible
- AWS CloudFormation
- Azure Resource Manager (ARM)
- Docker
- Google Cloud Platform (GCP) Deployment Manager
- Helm
- JSON
- Kubernetes
- Terraform (for AWS, Azure, GCP, Kubernetes)
- XML
- YAML

DEVELOPMENT AND DEVOPS INTEGRATIONS

Source code management (SCM) systems

- GitHub
- GitLab
- Azure DevOps
- Bitbucket

- Concourse*
 - Sbt*
 - TeamCity*
 - Gradle*
 - Wind River Studio*
 - Travis CI*
- *Supported via the Black Duck Bridge CLI

Issue-trackers

- Jira
- Azure Boards
- GitHub Issues

Training platforms

- Secure Code Warrior

Build/CI tools

- GitHub Actions
- GitHub App
- GitLab CI
- Azure Pipelines
- Bitbucket Pipelines
- Jenkins
- AWS CodeBuild*
- Bamboo*
- CircleCI*
- CloudBees*
- CodeShip*

SBOM formats

- SPDX
- CycloneDX

Third-party tools (SCA and SAST)

- Android Lint (SAST)
- Brakeman (SAST)
- Black Duck Binary Analysis (SCA)
- Checkmarx (SAST)
- Clang (SAST)
- Clippy (SAST)
- CodePeer (SAST)

- Coverity® Static Analysis (SAST)
- CppCheck (SAST)
- DefenseCode ThunderScan (SAST)
- Dependency-Check (SCA)
- ErrCheck (SAST)
- Error-prone (SAST)
- ESLint (SAST)
- Fortify (SAST)
- FxCop (SAST)
- Gendarme (SAST)
- Gitlab Security (SAST)
- GoCyclo (SAST)
- GoLint (SAST)
- GoSec (SAST)
- HCL AppScan Source (SAST)
- HCL AppScan on Cloud (ASOC) (SAST and SCA)
- Helix QAC (SAST)
- IneffAssign (SAST)
- JFrog Xray (SCA)
- JLint (SAST)
- Microsoft Code Analysis (SAST)
- MobSF (SAST)
- MobSF Scan (SAST)
- NDepend (SAST)

Third-party tools (SCA and SAST) continued

- OCLint (SAST)
- Parasoft JTest / C++Test / dotTest (SAST)
- PHP_CodeSniffer (SAST)
- PHPMD (SAST)
- PMD (SAST)
- Pylint (SAST)
- Rapid Scan SAST (Sigma) (SAST)
- Retire.js (SCA)
- SafeSQL (SAST)
- SARIF (SAST)
- SATE (SAST)
- Scalastyle (SAST)
- SCARF (SAST)
- SciTools Understand (SAST)
- Semgrep (SAST)
- Snyk Open Source (SCA)
- SonarQube Generic Issue Import Format (SAST)
- SpotBugs / FindBugs (SAST)
- Software Risk Manager™ (SAST and SCA)
- Staticcheck (SAST)
- TFLint (SAST)
- TruffleHog (SAST)
- Veracode (SAST and SCA)
- Vet (SAST)
- WPSan (SCA)
- ZPA (SAST)

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.