

Black Duck Expands Polaris Integrations to Deliver Frictionless DevSecOps at Enterprise Scale

Enhanced SCM integrations streamline automated repo onboarding, continuous monitoring, and event-based scanning across GitHub, GitLab, Azure DevOps, and Bitbucket

BURLINGTON, Mass., Feb. 12, 2026 /PRNewswire/ -- [Black Duck®](#), the leader in AI-powered application security, today announced the immediate availability of a powerful set of enhanced [Black Duck Polaris™ Platform](#) integrations across all major source code management (SCM) platforms — including GitHub, GitLab, Azure DevOps, and Bitbucket. The Polaris Platform is an integrated, software-as-a-service application security platform powered by the industry's leading static application security testing, software composition analysis, and dynamic application security testing engines.

With development teams managing an explosion of human and AI-generated code and increasingly distributed development environments, manual onboarding and fragmented security tools create serious coverage gaps. These enhanced Polaris capabilities enable organizations to achieve unprecedented speed, coverage, and automation in securing their applications at scale.

Designed for enterprises managing hundreds and even thousands of code repositories across globally distributed teams, these integrations dramatically simplify onboarding, accelerate scanning workflows, and seamlessly embed security into day-to-day development activities. Together, these enhancements reduce administrative overhead, eliminate manual configuration, and ensure continuous coverage for fast-changing codebases.

Key Features and Benefits:

- **Unified coverage across all major SCMs.** Whether teams use GitHub, GitLab, Azure DevOps, Bitbucket, or a mix of all four, the natively built integration with the Polaris Platform provides a consistent, unified security experience—not a scripted add-on.
- **Instant onboarding for thousands of repositories.** Organizations can automatically onboard and continuously synchronize Polaris with every repository in their SCMs without the need for manual configuration.
- **Continuous monitoring of repository changes.** New repositories, renamed projects, branch creation, and other structural changes are detected instantly, ensuring security coverage always remains current and complete.
- **Trigger scans on key development events.** Polaris scans can be triggered automatically when a pull request is created/updated or before it is merged—allowing developers to catch and fix vulnerabilities during their normal code review process—resulting in vulnerabilities being addressed earlier in the SDLC.
- **Apply AI-powered application security with Black Duck Signal™.** Enabling scans directly in the IDE or automated through CI/CD, all centrally managed in Polaris. Signal surfaces meaningful security insights in both human- and AI-generated code, helping teams stop vulnerabilities before code is committed.
- **Extend security and AI insights directly to the developer's desktop with Code Sight™.** This IDE plugin triggers Polaris scans—manually or automatically—while developers code. Combined with Black Duck Assist's AI-driven guidance and remediation, developers get immediate, actionable feedback, reducing

friction and preventing rework later in the lifecycle.

- **Customizable scanning with full or rapid analysis.** Teams can choose between deep, comprehensive scanning or ultrafast rapid analysis based on the context of each workflow.
- **Seamless integration into developer workflows.** Security findings surface directly inside pull requests, enabling developers to fix issues in real time—without switching tools or breaking flow.
- **Instant policy onboarding.** Enterprise security policies and guardrails can be enabled with a single click, ensuring consistent enforcement across thousands of repositories.
- **Instant user onboarding.** Teams, roles, and access controls synchronize automatically, reducing administrative overhead and accelerating time to value.

"Today's enterprises are orchestrating software projects across hundreds and thousands of source code repositories in the race to adopt AI in production," said Dipto Chakravarty, Chief Product and Technology Officer at Black Duck. "Development and Security teams need application security that is integrated, automated, and frictionless across their platforms and code repositories. No other solution combines the breadth of SCM platform support with universal event and policy-based automation, and the depth of analysis and agentic AI scalability provided by the Black Duck Polaris Platform. This is a game changer for operating DevSecOps at enterprise scale."

Availability

These enhanced integrations are available now for all existing customers and can be activated directly in Polaris Platform settings.

To explore these capabilities in depth—including demos and recommended implementation paths—read our [blog post](#), watch our [webinar](#) or [visit our website](#).

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.

SOURCE Black Duck Software

For further information: Liz Samet, Black Duck, 336.414.6753, esamet@blackduck.com

<https://news.blackduck.com/2026-02-12-Black-Duck-Expands-Polaris-Integrations-to-Deliver-Frictionless-DevSecOps-at-Enterprise-Scale>