Software Risk Manager

Simplify AppSec program management at enterprise scale

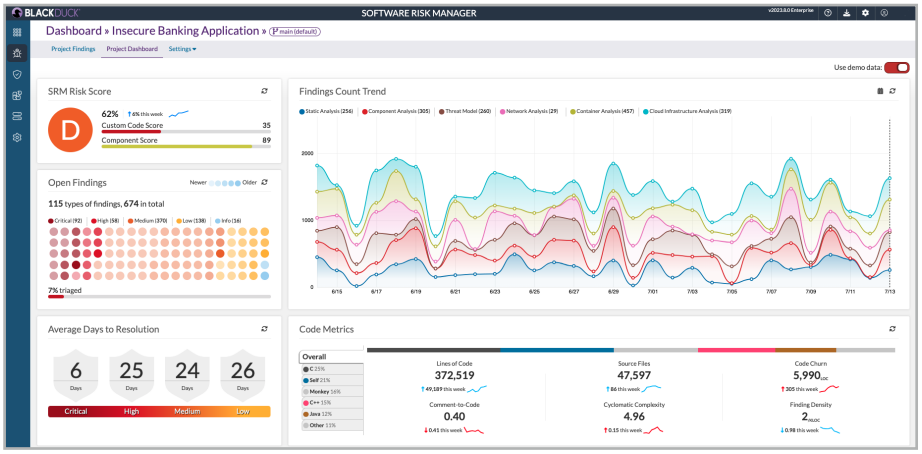
Overview

Black Duck Software Risk Manager™ is an on-premises application security posture management (ASPM) solution that enables security and development teams to simplify their application security programs to improve risk posture. It brings together policy, orchestration, issue correlation, and built-in static application security testing (SAST) and software composition analysis (SCA) engines to integrate security activities intelligently and consistently across the software development life cycle (SDLC). With Software Risk Manager, security and development teams can make informed decisions from a single source of truth and deliver resilient applications at scale.

Eliminate silos and gain actionable insight with Software Risk Manager

By introducing transparency, efficiency, and accountability to application security (AppSec) workflows, Software Risk Manager provides the necessary foundation to integrate checks at every stage of the SDLC. Software Risk Manager offers key capabilities to scale testing, remediation, and risk management.

- Integration with 150+ security and developer tools—more than any ASPM solution on the market today
- Centralized policy management
- Built-in testing engines for industry-leading Black Duck SAST and SCA
- Support for 20+ compliance standards
- Customizable, extensible correlation rules
- Bidirectional integration with popular issue-trackers and developer tools including Jira, ServiceNow, Azure DevOps, GitLab, GitHub, Jenkins, TeamCity, and Bamboo, as well as IDE plugins for Visual Studio, Eclipse, Visual Studio Code, and IntelliJ
- Sixteen built-in open source testing tools—the correct tool is automatically recommended via language detection



Application security findings and performance metrics displayed on the Software Risk Manager dashboard

Key benefits

Consolidate AppSec with a central system of record

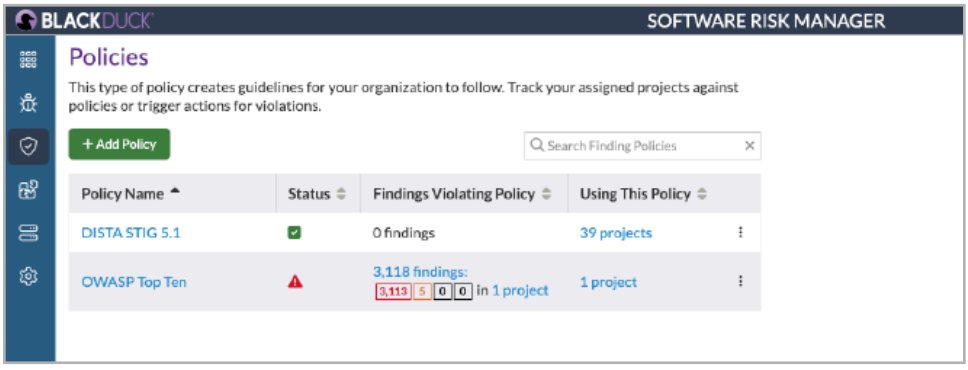
- Feeds all findings across manual and automated testing into a system of record that tracks all AppSec testing activities, security data, and policies, providing granular visibility of your application security posture at every stage of the SDLC
- Automatically correlates and deduplicates results from disparate testing sources, providing a unified user experience and making it easier to view and prioritize issues
- Supports the most commonly used security testing tools including SAST, SCA, dynamic application security testing, interactive application security testing, InfraSec, and threat modeling, as well as testing for mobile, containers, and cloud infrastructure
- Automatically selects the best available AppSec tools for your codebase
- Dynamically discovers SCM repositories, applications and associated developers and security users through automated onboarding for built-in SAST and SCA

Accelerate triage, testing, and remediation workflows

- Automatically identifies and prioritizes critical issues based on a uniform assessment of risk
- Delivers high-priority vulnerabilities to developers directly, including links to the exact line of code via bidirectional sync with issue-tracking systems
- Quickly and accurately detects vulnerabilities in source code and open source via built-in SAST and SCA engines, with preset rules to achieve required testing workflows with minimal setup
- Provides contextually relevant remediation guidance to developers based on language, vulnerability type, and source, and recommends remediation actions based on historical trends
- Displays security activities at the branch level, enabling efficient testing for fixes and reducing the frequency of build breaks
- Centrally orchestrates scans for Black Duck tools (built-in or standalone) or third-party tools

Centralize risk visibility and governance

- Provides a 360-degree view of risk scoring, findings, and key performance trends for all projects and sources of code (custom built, third party, and open source)
- Maps findings to regulatory compliance standards (including NIST, PCI, HIPAA, DISA, OWASP Top 10) and provides audit reports for critical violations
- Provides both UI and API-based workflows to create, enforce, and monitor security policies across software assets and components
- Enables security teams to specify risk thresholds for issue types, desired application security testing tooling, SLAs on remediation time for fixes, and required notifications to development stakeholders



Findings that violate policies can be tracked by project, source, and criticality

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.