

The Black Duck Advantage: Application Security for the Federal Government

Black Duck tools enable secure modernization, with real-time visibility, automated testing, and centralized risk management. Federal civilian agencies and the Department of War (DoW) face a rapidly shifting and increasingly complex AppSec landscape. Regulatory expectations continue to evolve—driven by Executive Orders like President Trump’s 2025 cybersecurity directive, which mandates thorough audits of legacy systems and enforces stricter cybersecurity accountability across the federal enterprise. Agencies are being called to modernize aging infrastructure, adopt zero trust principles, and secure sprawling application portfolios—all while contending with limited budgets, persistent talent shortages, and escalating supply chain risks.

Real Results, Real Security

Black Duck delivers comprehensive application security solutions designed to meet the unique demands of federal environments—precisely why 11 civilian agencies and the top 10 aerospace and defense contractors rely on it for their AppSec needs. More specifically, Black Duck:

- 1. Centralizes Risk Management:** Consolidates proprietary source code, open source and third-party software risks into a single, unified view—empowering agencies to streamline oversight and reduce the operational burden of enabling teams on multiple tools.
- 2. Ensures Software Integrity Across All Sources:** Delivers robust protection whether software is developed in-house, outsourced, or acquired commercially.
- 3. Delivers Early, Actionable Intelligence:** Surfaces critical vulnerability data—exploits, workarounds, and remediation guidance—quickly and in a digestible format, often weeks before listings appear in the National Vulnerability Database (NVD).
- 4. Aligns with Federal Security Standards and Compliance:** Supports key frameworks including NIST 800-53, NIST 800-171, the NIST Secure Software Development Framework (SSDF), the upcoming NIST Cybersecurity Supply Chain Risk Management (C-SCRM) guidance, FISMA, CISA’s Zero Trust Maturity Model (ZTMM), and the continuous monitoring required of a cATO.
- 5. Integrates Secure Coding into Developer Workflows:** Offers in-context training and remediation guidance that aligns with the SDLC—promoting secure coding practices without disrupting productivity.

The results are tangible. According to a recent survey, Black Duck customers have seen:

↓42%

reduction in time spent on manual code quality and security reviews

↓66%

decrease in average remediation time

↓75%

decrease in time spent preparing risk reports or performing security audits

↓55%

reduction in delayed releases due to security issues

Source: Black Duck Customer Value Study, 2025

True Scale Application Security

Black Duck has led the Gartner Magic Quadrant for Application Security Testing (AST) for seven years and is an accepted technology in Iron Bank, part of the DoW's Platform One. We're not just a vendor; we're a comprehensive security partner.

Our portfolio includes:

- **Software composition analysis (SCA)**, detects and manages open source and third-party component risks and produces the Software Bill of Materials required for supply chain initiatives and regulatory requirements.
- **Static application security testing (SAST)**, is the most trusted solution for finding code quality defects in applications of any size, and satisfying strict compliance standards.
- **Dynamic application security testing (DAST)**, safely and efficiently performs dynamic testing on production applications, testing software in the same state as attackers.
- **Interactive application security testing (IAST)**, offers unparalleled visibility into web app security and enables security teams to identify and track sensitive data to ensure that it is handled securely.
- **Application security posture management (ASPM)**, brings together policy, issue prioritization and remediation to deliver a centralized view of software risk for your organization.
- **OSS Snippet API**, Decreases the license risk associated with AI-generated code by analyzing snippets of open source before it even reaches the IDE.

Black Duck's extensive language and framework coverage is tailored to the complex environments of federal civilian agencies and the DoW. We support secure operations with FedRAMP-authorized deployment and compatibility with classified and air-gapped environments. For both government developers and defense contractors, Black Duck provides actionable remediation guidance for static and dynamic testing—backed by verified, mission-relevant security intelligence.

Get Started Today

AppSec cannot be an afterthought. Federal agencies and the DoW must be freed from tradeoffs between speed, accuracy, and compliance at scale. Ready to build secure-by-design systems that meet mission objectives and regulatory mandates? Get in touch today.

For more information, please visit blackduck.com