BLACK DUCK®

SOFTWARE SUPPLY CHAIN SERVICES

Properly managing software supply chains is complex, but with Black Duck Software Supply Chain Services, you can meet the emerging regulatory and governance requirements with confidence.

OVERVIEW

Legislation requiring stringent software security practices by software producers is being passed around the globe. This requires organizations to rethink their approach to software security, which industry standards they follow, and the best practices for their software development teams. While this legislation is often focused on the software procured by governmental departments, agencies, and contractors, the reach of such legislation has a direct impact on enterprise software, cloud services, and consumer level products. This turns governmental procurement from a simple transaction into one that has a much broader impact across critical infrastructure sectors and related technology suppliers.

One common component across the legislative efforts is the concept of "robust Software Bill of Materials (SBOM)" and participation in vulnerability disclosure programs. Software producers are increasingly expected to have a greater understanding of how their software is authored, tested, and secured. This includes maintaining up-to-date documentation outlining the origin of each software component, attesting to testing outcomes and risks mitigated during testing, and employing automated processes to maintain trusted software supply chains throughout the software life cycle. In addition, an SBOM offers a common framework for documenting and communicating an application's "ingredients" to reduce code opacity, particularly for third-party open source components.

SOFTWARE SUPPLY CHAIN SECURITY CHALLENGES

As with most new processes, there are challenges to securing the software supply chain within a given piece of software, regardless of whether your team created the software, contracted for its creation, or simply bought it from a software producer. Consider the question of component identification. Any system based off an assumption that there is a single source of software—the vendor—will fail to properly identify open source components. This is because there is no single vendor for open source software; instead, there are many contributors, each with their own origin point where anyone can download the software. Correctly identifying these disparate locations remains an unsolved industry problem, and it will require the use of a standard nomenclature for each component, regardless of how it was developed. Once a component is identified, development communities and ecosystems will need to work collectively on standards, processes, education, and tooling to mitigate the risks related to usage of third-party code within an application.

SBOMs are a technical solution to business problems. Building trust within a software supply chain requires transparency in software composition and conformance to recognized standards like the NIST Secure Software Development Framework.

Most people investigating software supply chain risks will encounter standard SBOM formats such as Software Package Data Exchange (SPDX) and CycloneDX—two SBOM standards accepted by the NTIA as meeting the requirements for an SBOM. These standards are designed to help companies easily exchange information related to the usage of third-party software in an application and help build trust and transparency in how software is created, distributed, and consumed throughout supply chains. But the SBOM market is still immature. And although these standards help companies exchange information, they don't address issues of the completeness and accuracy of the data contained with an SBOM document.

SECURING YOUR SUPPLY CHAIN WITH BLACK DUCK SERVICES

SSDF Readiness Assessment

The National Institutes of Standards and Technology (NIST) has produced guidance known as the Secure Software Development Framework (SSDF). The SSDF presents a series of practices and associated tasks that serve as a baseline for teams seeking to securely develop software in a standardized way. Attestation to conformance with a subset of the SSDF has been signaled by the U.S. government as a requirement for all software procured directly or indirectly by the U.S. government and produced after September 2022, and that is subject to continuous update, and software suppliers will need to self-attest to their adherence to the SSDF.

The Black Duck® SSDF Readiness Assessment identifies whether your organization's software development practices align with the practices and tasks of the SSDF. It then provides an assessment of which controls are lacking for conformance with guidelines. This assessment, and associated corrective recommendations, can be used when completing U.S. government attestations.

SBOM Management Maturity Action Plan

Creating an accurate and complete SBOM often requires more than pointing an SBOM generation tool at source code and generating an SBOM. The SBOM Management Maturity Action Plan (MAP) from Black Duck provides software security leaders and practitioners with actionable guidance to reliably produce SBOMs for their customers, and it provides guidance on how to consume the SBOMs received by from their suppliers. It also assesses an organization's people, processes, and technology involved in generating an SBOM to ensure that it is accurate and conforms to SPDX or CycloneDX standards.

SBOM Generation as Audit Service

Software producers will have requirements to generate an SBOM for regulatory or contractual reasons, and the penalty for an inaccurate or incomplete SBOM can be severe. Building upon the proven Black Duck® Audit Services processes, the Black Duck Audit Services team performs a full security audit of the software and then generates an SBOM meeting the minimum data requirements for the desired SBOM. The SBOM-generation-as-an-audit service offering is particularly valuable if you do not have SBOM generation capabilities and want a proven baseline SBOM for your applications.

SBOM Audit and Validation

Software producers with regulatory or contractual SBOM requirements and that generate their SBOMs using automation may face a request for an audited SBOM. Similarly, software consumers might want to audit the SBOM produced by one of their suppliers. In each of these scenarios, a trusted third party with a strong reputation in software audits is required. Black Duck Audit Services software security audits are the gold standard for technical due diligence security reviews during a merger or acquisition process. The Black Duck SBOM Audit and Validation service builds on those proven processes to audit the software and confirm whether the SBOM produced by client automation accurately reflects the supply chain.

Secure DevOps Pipeline Assessment

Without a secure DevOps pipeline, any attestations made based on pipeline actions are questionable . The Secure DevOps Pipeline Assessment from Black Duck provides a reference set of controls to validate the security of a DevOps pipeline and associated infrastructure. Example strategies include access control, network security, encryption, auditing, and continuous monitoring.

Key Benefits

Software producers have a critical role to play in securing software supply chains for the benefit of their customers and users. With Black Duck software supply chain services, you can

- Verify and attest with confidence that your software development processes conform to SSDF standards
- Meet regulatory requirements by generating a standard-format SBOM without allocating your valuable security resources
- Identify the software supply chain security and SBOM strategies, capabilities, and activities your organization should employ
- Ensure that your SBOM and SBOM generation tools and processes are accurate and complete with third-party expert validation and guidance
- Validate the security, configuration, and processes utilized within your DevOps pipeline

Take advantage of our 20+ years of experience implementing successful software security programs. Black Duck can help develop your software supply chain security strategy, and then help you get the buy-in, resources, and support you need to implement it.

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.