BLACK DUCK OPEN SOURCE AUDITS

PURPOSE-BUILT FOR M&A

Solidify your approach to open source due diligence with an understanding of the differences between open source management tools and open source audits for M&A.

OVERVIEW

Merger and acquisition (M&A) due diligence is a high-stakes process. There's little margin for error or waste in any of the analyses that are part of due diligence; accuracy, expertise, and clear, timely results matter. And when it comes to open source diligence, an acquirer needs to choose an approach tailored to meet those strict demands.

Auditing code for open source software components and their associated licenses and security vulnerabilities in M&A requires a different approach than most scan tools can accommodate. That's why choosing a solution purpose-built for M&A ensures the deal team gets the answers they need in time to move forward confidently.

Typically, target companies in an M&A deal aren't comfortable handing over the underlying code of the software asset at the heart of the deal to acquirers. But neither do they have an accurate picture of what open source components are in their code. Deal teams who turn to a third party to audit software applications for open source see these benefits:

- **Trust and speed.** Targets can trust a third party with their code, acquirers can trust them to be thorough, and the third-party team can ensure that the audit moves at the speed of M&A.
- **Accuracy.** An open source software audit provides a complete picture of all open source in the application.
- **Expertise.** A third-party audit team consists of open source experts with decades of experience analyzing software.
- **Insight.** Audit deliverables include reports that are detailed, easy to consume, and easy to share.

"When we make an acquisition, we use a variety of Black Duck Audit Services, which has allowed us to consolidate the third-party requirements into one vendor and one solution. That has made it a lot easier to understand the risks before we bring new technology into our portfolio."

—PointClickCare

TRUST AND SPEED

At the heart of a technology transaction is, of course, the technology. The target is not always willing to hand over their IP for inspection before a deal is done. In that case, a third party can operate between the target and the acquirer. For the target, the third party ensures IP is protected and handled properly; for the acquirer, the third party provides an unbiased analysis of the asset.

M&A moves fast, and diligence is no different. When the clock starts, both teams need to ensure that complete and accurate analysis happens in a timeframe that accommodates the deal. Given the massive scope that diligence covers, using a third party to handle certain aspects helps M&A teams meet these aggressive timelines.

ACCURACY

A key element of an open source audit is making sure the results of scanning software are accurate and thorough. Companies often find open source hidden in their code that they didn't know was there. Even the most open and straightforward deals can be unknowingly affected by open source.

Black Duck® open source audits are purpose-built for M&A scenarios. To augment our deep expertise, the Black Duck Audit team uses multiple tools and techniques, including in-house, third-party, and homegrown technology that they've tuned through decades of open source experience.

Deep discovery and analysis

The audit team uses multiple techniques to identify open source in software applications. They use Black Duck's extensive KnowledgeBase™ to match open source components found in the code. In the absence of source code, they match binaries. They also identify full open source components pulled in, and can scan file systems for directory metadata to discover undeclared, modified, and partial open source components.

From there, the audit team uses snippet analysis to find even small pieces of open source in a codebase. An example of snippet use is when a developer copies a few lines of code from an open source component because that's all they need. Because they don't use the entire component, most open source scan tools can't detect it.

In terms of security, the chances that a vulnerability affects that snippet of code are low. However, the presence of that snippet still requires the licensee to comply with the associated license. And copyleft licenses can require that the licensee freely distribute the entire codebase in which the snippet is used, which is problematic and puts the IP at the center of an M&A deal at risk. Thus, the acquiring company needs to discover every snippet of code in the target's software to ensure it can be used free and clear.

String search

The Black Duck Audit team uses string searching to discover easy-to-miss pieces of open source or essential information found in software. String searching is a key part of our software audits for two important reasons. The first is the capability itself, which allows us to build logic into our search for open source—for example, "Search for a string that includes the word 'copyright' within five words of the word 'incorporated' but does not include *target company name.*" This capability uncovers copyrights in the software that may not belong to the target. It also discovers references such as URLs that can identify code pulled from blogs, custom licenses, or code that requires a commercial license. The second reason is that the Black Duck team has years of experience performing audits and has developed a sophisticated and comprehensive collection of targeted string searches that nets results that others miss.

Potential BOM inaccuracies and why the use case matters

As you can imagine, going to this level of detail produces an extensive software Bill of Materials (SBOM). When the search for open source is a mile wide and a mile deep, it is likely to produce a long list of findings that require additional vetting. An automated scan tool, even one like Black Duck's tool (which, unlike most, can discover open source snippets), is still just that—an automated tool. To create the most accurate SBOM, experts must review the results of any automated scans.

Typically, in an M&A scenario, the team managing due diligence faces two constraints: time and a lack of subject matter expertise. Potential deals are often highly sensitive, and deal teams are kept intentionally small—so they rarely contain enough subject matter expertise across every facet of tech diligence to analyze open source results at this level. Adding to that, diligence timelines are often extremely tight, cramming months of person-hours into mere weeks. With tight resources and timelines, it's a best practice to defer to third-party expertise to scale the process.

EXPERTISE

The audit team's combination of in-depth scanning technology and decades of open source experience results in the most accurate and thorough open source analysis possible.

Another benefit of using a third party to perform an open source audit for M&A is access to a team of open source experts to analyze the audit results. Black Duck consultants have decades of experience and analyze open source full-time. They recognize file names, understand what open source is common and where it's commonly used, and pick up on nuances that only experience can reveal. This expertise is essential in reviewing open source components, as it helps them get to the correct result quickly.

Further, the team, with their extensive open source experience, has assembled its own set of best-in-class tools to help them discover and analyze open source. The team has developed hundreds of string search expressions, uses a tool to analyze build files, and can look at a side-by-side comparison of open source snippets found in the code alongside any hits in our KnowledgeBase. There's just no match for experienced auditors who look at open source for a living and what they're able to interpret. And when they encounter an inconclusive result, such as a component flagged as "unlicensed," they take the time to research and make sure nothing was missed.

This combination of in-depth scanning technology and the audit team's decades of open source experience results in the most accurate and thorough open source analysis possible.

INSIGHT

Finally, when your diligence team is moving fast toward a buy/no-buy decision, it's important to receive results in a consumable, sharable, informative format. A Black Duck Audit delivers a set of reports written by the auditors who performed the analysis. It includes an executive summary, which can be passed along to the deal sponsors, outlining any risks that were found, as well as a detailed open source risk report and a spreadsheet containing a full SBOM, associated licenses, potential security vulnerabilities, and enhanced vulnerability data that details the vulnerability and a path toward remediation. The reports are easy to consume and share, and they provide the team with a full picture of the open source in a codebase—all within a timeframe that works in M&A.

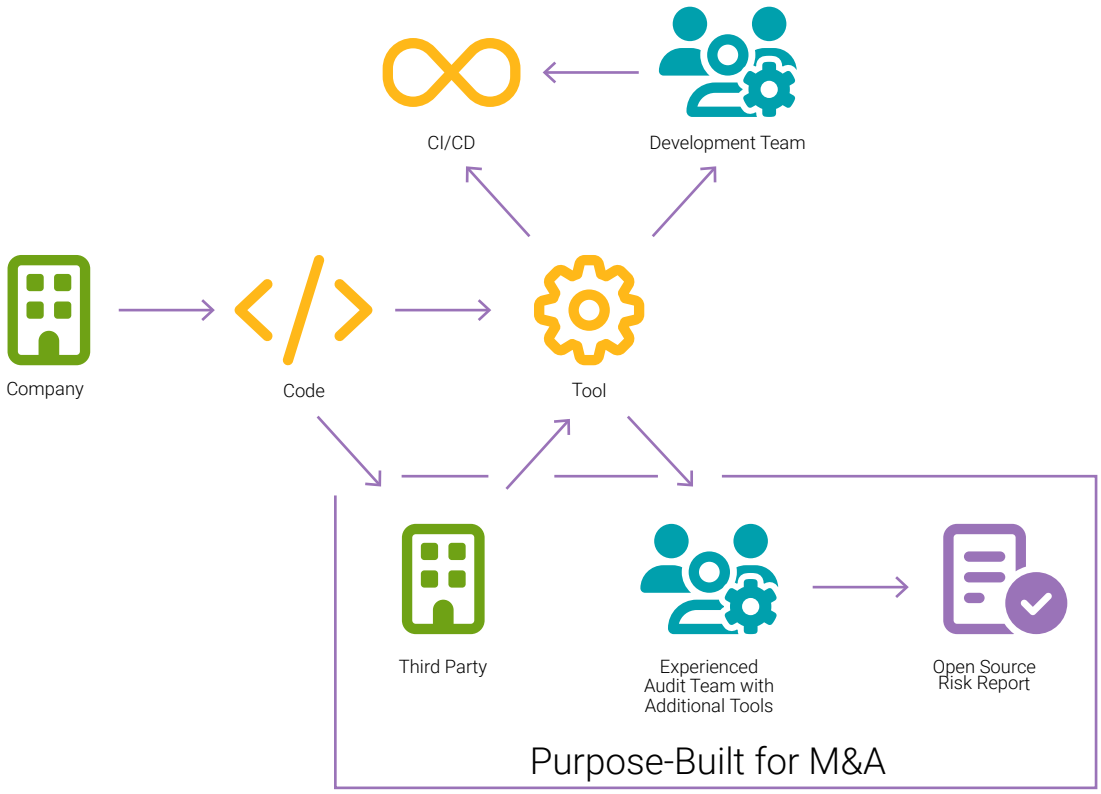
WHY THIRD-PARTY OPEN SOURCE AUDITING IS BEST IN M&A

Development and security teams need open source management tools so they can integrate and automate open source management in their software development life cycle. It's what those tools are built and optimized for and what they do best. In fact, such tools depend on data from the build system for optimal results.

But when M&A is in motion and tech diligence is underway, an acquirer can't use such tools to get accurate results in a fast-enough timeframe—not without building new tooling to analyze software in "offline" mode (i.e., not integrated with the build system), and not without the experience to interpret the results.

When it comes to open source auditing for M&A, there is a clear advantage to hiring a third-party team that

- Can build the trust needed for the target company to upload the source code for analysis
- Has the tools and expertise to find all the open source in the software
- Contains the in-house expertise to analyze results for accuracy and take the analysis deeper than an automated tool could
- Can move with the speed required of M&A transactions
- Produces the reports that stakeholders need to make the most informed decision possible—whether that's buy/no-buy, valuation changes, escrow funds, or integration timelines and expenses if the deal moves forward



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.