Automate Attribution Fulfillment via Third-Party Notices Generation

Create Third-Party Notices with the Click of a Button

Organizations today have to take into account the amount of open source software (OSS) being utilized in order to develop an effective strategy for maintaining the compliance and security of the software supply chain. In many cases, it comprises upwards of 70 percent of the code. Development teams recognize that the benefits far outweigh the risks—quicker time to market, higher levels of innovation, and lower cost of ownership. In some cases, not highly leveraging open source in the development process could be a competitive *disadvantage.*

When open source components are used, however, that code is authored by individuals who licenses the use of the code to others. Licenses vary and subsequently so do the legal obligations of the user. Attribution for the author is one of those necessary obligations.

To help companies remain compliant and provide legally required attribution, Code Insight from Revenera automatically satisfies this requirement by generating complete third-party notices with just the push of a button.

Create Complete Third-Party Notices for All Components

OSS licenses are legal and binding contracts between the authors and the users of a software component, declaring how software can be used and under what specified conditions. The license is what determines how to abide by the authors' wishes. Without an open source license, the software component is often unusable by others due to the ambiguity around its proper use.

KEY FACTS:

- Revenera is the leader in providing complete third-party notice attribution for open source code
- Provides automated, push-button third-party notice report generation, including the production of SBOMs
- Eliminates time-consuming manual effort of identifying and collecting actual license texts related to open source components identified in applications
- Enables organizations to be compliant with the attribution requirement which is one of the most common license obligations
- Eliminates potential legal action due to unfulfilled license obligations
- Most complete and up-to-date library of actual license texts associated with open source component versions

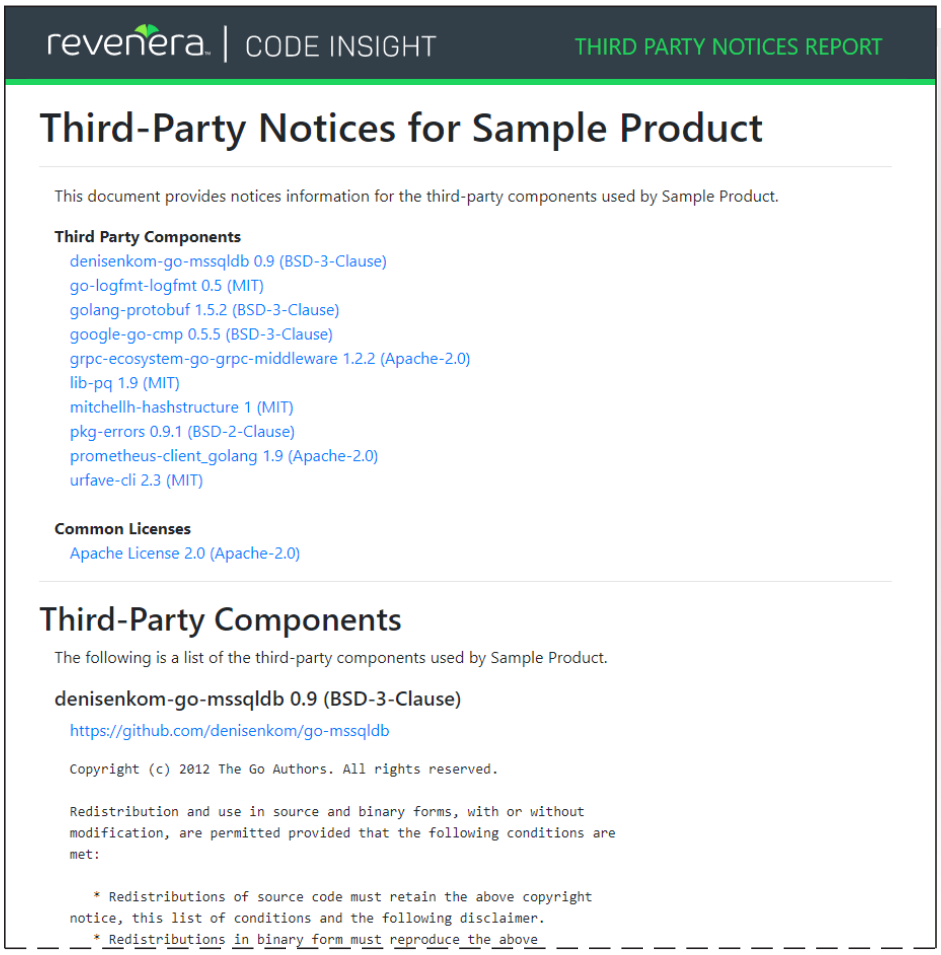
The license text provides a complete explanation of any requirements and/or restrictions for the use of a given component and often includes the main copyright statements. For example, some questions answered include:

- Can the code be utilized in commercial software?
- Is the code only to be used in free and open source software?
- Can the code be modified?
- What type of modifications are permitted?
- How should author attribution be declared?
- Which uses are prohibited?

Code Insight allows users to automatically generate third-party notices for open source and third-party components. Our extensive library provides extensive coverage of the most popular components and their associated licenses, regardless of version. And, we are collecting license text information on an ongoing basis.

Generating a report through Code Insight at the click of a button eliminates countless hours of manual time-consuming effort of identifying and collecting actual license texts governing the use of the open source components in applications. Development teams can generate a third-party notice report in the format of their choice and include in as part of their compliance artifacts per whatever internal process they follow.

SAMPLE THIRD-PARTY NOTICE REPORT FROM CODE INSIGHT



revenera | CODE INSIGHT THIRD PARTY NOTICES REPORT

Third-Party Notices for Sample Product

This document provides notices information for the third-party components used by Sample Product.

Third Party Components

denisenkom-go-mssqldb 0.9 (BSD-3-Clause)
go-logfmt-logfmt 0.5 (MIT)
golang-protobuf 1.5.2 (BSD-3-Clause)
google-go-cmp 0.5.5 (BSD-3-Clause)
grpc-ecosystem-go-grpc-middleware 1.2.2 (Apache-2.0)
lib-pq 1.9 (MIT)
mitchellh-hashstructure 1 (MIT)
pkg-errors 0.9.1 (BSD-2-Clause)
prometheus-client_golang 1.9 (Apache-2.0)
urfave-cli 2.3 (MIT)

Common Licenses

Apache License 2.0 (Apache-2.0)

Third-Party Components

The following is a list of the third-party components used by Sample Product.

denisenkom-go-mssqldb 0.9 (BSD-3-Clause)

https://github.com/denisenkom/go-mssqldb

```
Copyright (c) 2012 The Go Authors. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are
met:

   * Redistributions of source code must retain the above copyright
notice, this list of conditions and the following disclaimer.
   * Redistributions in binary form must reproduce the above
```

The Relationship Between SBOMs and Third-Party Notices in Code Insight

An SBOM is a catalog of software parts (OSS/third-party/commercial) in your application. Third-party notices are attributions to all of the third-party code in a product—a lower-level view of external contributions to a product.

Code Insight from Revenera supports the management of these two things. Meaning, most companies today are driven by the need to produce SBOMs for their supply chain partners and to support their application security risk management strategy. Given that, the natural starting point is an application's SBOM. Code Insight supports the construction of an SBOM via a combination of import, manual disclosures, and scanning.

Organizations producing software essentially have two options:

- Use a freely available industry tool to convert the SBOM to a starter notices file with component, version, and license names. However, the remaining manual work is to find the actual license text and copyright statements for each component version and incorporate them into the third-party notices report. This is typically done by an internal legal team or an outside consulting or legal agency.
- Code Insight offers support to ingest an SBOM, automatically add in the actual license text from the Revenera data library, and produce a third-party notices report. Optionally, Code Insight provides support for further building out the SBOM via deep scan and/or manual analysis capabilities down to the fragment of code.

Continuous Open Source Compliance

Managing the complexities of the entire software supply chain makes license compliance burdensome, complex, and time consuming for engineering leaders and software developers. With Revenera's automated attribution, users protect their intellectual property from legal risk and empower engineering teams with faster, more compliant software development.

NEXT STEPS

Visit us to learn more about your open source license compliance obligations.

LEARN MORE >

Revenera provides the enabling technology to take products to market fast, unlock the value of your IP and accelerate revenue growth—from the edge to the cloud. **www.revenera.com**