SYNOPSYS®

Black Duck Web Services and API Risk Audit

Get the information you need to know about the web services used in your—or your target company's—code

Overview

Applications today not only comprise open source and proprietary code but also use tens of thousands of external web services that are called through APIs. These web services are easy for developers to get, typically free, and often not formally tracked by the company. For example, a developer could use the Google Maps API to pass latitude/longitude data and get time zone information to display in an application. These types of web services can quickly multiply in the codebase. Tracking them, and their associated obligations and data risks, can become cumbersome. As with open source, most companies simply don't know what web services their applications depend on.

The growth and pervasiveness of open source in commercial code have made it an integral part of the need for understanding and protecting intellectual property. Getting to the root of potential risks associated with open source ahead of an event—be it acquisition, investment, divestiture, or funding—is paramount to protecting IP value. But what about the other third-party services that could have made their way into your code and present additional unknown risks?

As with open source, companies often have little visibility into the web service APIs on which their applications depend. Those applications may have problematic terms of service associated with them, and the terms of service can be changed frequently and without notice. Web services can also expose your company to potential data privacy or overall operational risks that could disrupt or severely impact your business.

Web services can expose your business to potential license, data privacy, or overall operational risks that could disrupt or severely impact your business

Challenges with using web services

Governance risk

- **Terms of service change frequently and without notice.** Often implicit is that continued use equals acceptance of new or changed terms.
- **Terms can perpetually link to other terms,** making a never-ending agreement that is difficult to track and understand.

Data privacy risk

- **Data breaches can compromise personal data.** Web services can be susceptible to man-in-the-middle attacks meant to spoof servers and obtain sensitive information, especially if unencrypted. For example, the GitHub API was a victim of a man-in-the-middle attack.
- **You can't control the usage and privacy of personal data.** You don't always know the geographic location of the web service and whether sensitive data is going to undesirable locations. Passing data to these APIs could put you at risk of violating regulations such as GDPR or Safe Harbor.

Operational risk

- **Web services can be disrupted or discontinued.** An API can be shut down without notice, causing major disruptions if it is an integral part of your application.
- **You might unintentionally be using unreliable web services.** Not every web service is reliable. Issues with performance or uptime could create a negative experience for your users.

The Black Duck Web Services and API Risk Audit scans the code to generate a list of external web services used by an application. Further, it calls out web services that may introduce legal or privacy risk into your application. The extensive API KnowledgeBase™ behind the scan contains over 15,000 web services, 10,000 providers, 50 categories, 30,000 terms of service, and 30 legal acts for a comprehensive view of what's in your code. Through a summary report, you will be able to quickly determine your risk across key categories:

Governance risk

- Identifies the terms of service per API
- Identifies the legal acts or regulations related to the terms of service
- Tracks the frequency of changes in the terms

Data privacy risk

- Identifies the category of data passed in the API
- Classifies the type of authentication the API uses
- Pinpoints the API's geographic origin

Operational risk

Your team can use the API BoM (see below), combined with an evaluation of how integral these APIs are to your applications, to assess this area of risk.

Additional information

You'll also receive a detailed appendix so you can fully understand the external web services in your applications. The appendix is cut into different views depending on your focus:

- **Legal agreements in use.** Lists legal agreements and the APIs in which they are referenced. Legal agreement URLs link directly to related documents.
- **API bill of materials (BoM)**. Lists web service APIs with their metadata and risk. Includes API names, providers, categories, authentication methods, privacy risk, governance risk, the number of API matches, and the number of legal agreements found.
- **Identified files.** Lists files where web service API references were found, along with API names and specific identified URL references.

Black Duck Web Services and API Risk Audits help you get your arms around the external web services in your source code, using over a decade of expert knowledge to provide you with the information you need to know about in your—or your target company's—code.

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

For more information, go to www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com

SYNOPSYS®
Silicon to Software™

03/27/19.ds-bd-odwebaudit.